


ADVERTIMENT. L'accés als continguts d'aquesta tesi queda condicionat a l'acceptació de les condicions d'ús establertes per la següent llicència Creative Commons:  <https://creativecommons.org/licenses/?lang=ca>

ADVERTENCIA. El acceso a los contenidos de esta tesis queda condicionado a la aceptación de las condiciones de uso establecidas por la siguiente licencia Creative Commons:  <https://creativecommons.org/licenses/?lang=es>

WARNING. The access to the contents of this doctoral thesis it is limited to the acceptance of the use conditions set by the following Creative Commons license:  <https://creativecommons.org/licenses/?lang=en>



Universitat Autònoma
de Barcelona

Doctoral Thesis

Doctoral Program in Law- Institute of Law and
Technology

Faculty of Law

2024

Data Protection Law Aspects of Spanish and European
Contact Tracing Applications: Assessing Risks, Their
Compliance and Proposing Mitigation Strategies

Name of the Candidate: R. Baran Tombul

Name of the Director: Dr. Antoni Roig Batalla

Contents

INTRODUCTION.....	10
PART I	25
CONTACT TRACING APPLICATIONS AND THEIR POTENTIAL THREAT TO DATA PROTECTION.....	25
I. THE MAIN FEATURES OF CONTACT TRACING APPLICATIONS	26
1. General Framework	26
1.1 PURPOSE	26
1.2 CLASSIFICATION OF DIGITAL APPLICATIONS USED IN COVID-19	27
1.3 USE CASES ACROSS THE WORLD REGARDING THEIR IMPLEMENTATION OF THE APPLICATIONS	30
2. Location or proximity contact tracing.....	36
3. Architecture of the Applications.....	42
4. Pseudonymization and Anonymization	52
5. Data Storage and Management.....	57
6. Obligation to Use Contact Tracing Applications	63
7. Transparency and Accountability of the Contact Tracing Applications	67
II.- DATA PROTECTION RISKS AND CONCERNS ABOUT CONTACT TRACING APPLICATIONS	75
1. GENERAL DIGITAL CONTACT TRACING RISKS	75
2. LOCATION AND PROXIMITY RISKS.....	79
3. ARCHITECTURE RISKS	88
4. PSEUDONYMIZATION AND ANONYMIZATION RISKS.....	96
5. DATA STORAGE AND MANAGEMENT RISKS	102
6. OBLIGATORY USE RISKS.....	115
7. TRANSPARENCY AND ACCOUNTABILITY RISKS	120
PART TWO- EUROPEAN REGULATORY FRAMEWORK FOR CONTACT TRACING APPLICATIONS	133

III- LEGAL BASIS, GENERAL GDPR PRINCIPLES AND DATA SUBJECT RIGHTS UNDER THE GDPR	134
1. GDPR PRINCIPLES AND CONTACT TRACING APPLICATIONS.....	134
2.CONCRETE RECOMMENDATIONS ON LEGAL BASIS OF PROCESSING, DATA MINIMIZATION, PURPOSE LIMITATION, CONSENT AND TRANSPARENCY REQUIREMENTS, AND DATA SUBJECT RIGHTS.....	136
2.1 LEGAL BASIS OF CONTACT TRACING APPLICATIONS	136
2.2 Data Minimization	148
2.3 Purpose Limitation.....	160
2.4 Consent Requirement:.....	170
2.5 NOTICE, TRANSPARENCY AND ACCOUNTABILITY REQUIREMENT	179
2.6 DATA SUBJECT RIGHTS.....	191
IV- CONTROLLER/PROCESSOR OBLIGATIONS UNDER THE GDPR.....	206
1. Processing of Location data	206
2. Security of Processing, Accuracy, Integrity, and Confidentiality	218
3. DPIA REQUIREMENT	234
4. Privacy-by-design:.....	247
5. Privacy by default	258
V- EUROPEAN UNION GUIDELINES AND DOCUMENTS ON CONTACT TRACING	270
1. GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK.....	272
2. EU TOOLBOX FOR CONTACT TRACING APPLICATIONS (EHEALTH NETWORK)	290
3. Communication From The Commission - Guidance On Apps Supporting The Fight Against COVID 19 Pandemic In Relation To Data Protection (2020/C 124 I/01)	300
4. COMMISSION RECOMMENDATION (EU) 2020/518 OF 8 APRIL 2020 ON A COMMON UNION TOOLBOX FOR THE USE OF TECHNOLOGY AND DATA TO COMBAT AND EXIT FROM THE COVID-19 CRISIS, IN PARTICULAR CONCERNING MOBILE APPLICATIONS AND THE USE OF ANONYMIZED MOBILITY DATA	314
5. INTEROPERABILITY GUIDELINES EU.....	323

**PART III- GENERAL LEGAL ASPECTS OF PANDEMICS IN SPAIN,
RADAR COVID APPLICATION UNDER SPANISH DATA PROTECTION
LAW AND REGULATIONS: FEATURES, RISKS AND RESOLUTIONS. 338**

**VI. SPANISH REGULATION OF PANDEMIC AND CONTACT TRACING
APPLICATIONS 339**

**1. CONSTITUTIONAL COURT DECISION 148/2021 AND DECRETO DE ALARMA
463/2020 339**

2. NEED FOR A NEW HEALTH REGULATION OF PANDEMICS 358

3. LEGAL ORDERS ON ASISTENCIA COVID AND RADAR COVID..... 373

**4. IMPLEMENTATION OF DATA PROTECTION LAW NECESSITIES IN SPAIN DURING
THE PANDEMIC..... 389**

5. LAWFUL BASIS OF DATA PROCESSING ACTIVITIES BY THE APPLICATIONS. 406

VII. RADAR COVID AND DATA PROTECTION 419

**1. GENERAL OVERVIEW OF THE APPLICATIONS USED LOCALLY AND COMPARATIVE
ANALYSIS OF ASISTENCIA COVID-19 TO RADAR COVID..... 419**

1.1 GENERAL OVERVIEW OF THE LOCAL APPLICATIONS IN SPAIN 419

1.2 COMPARATIVE ANALYSIS OF ASISTENCIA COVID-19 TO RADAR COVID 422

2. IMPLEMENTATION OF RADAR COVID..... 431

3. SECURITY ISSUES OF RADAR COVID 446

4. AEPD RESOLUTIONS PS/00222/2021 AND PS/00223/2021..... 458

**5. LESSONS-LEARNED FOR FUTURE CONTACT TRACING APPLICATIONS IN SPAIN
AND CONCLUSIONS 480**

**5.1 LESSONS-LEARNED FOR FUTURE CONTACT TRACING APPLICATIONS IN
SPAIN AND CONCRETE RECOMMENDATIONS..... 481**

CONCLUSIONS 492

REFERENCES 500

Acknowledgements:

As I come to the culmination of my doctoral journey, I am filled with a profound sense of gratitude to all those who have supported and guided me along the way.

First and foremost, I would like to express my deepest gratitude to my thesis director, Prof. Antoni Roig Batalla, for his unwavering support, guidance, and expertise throughout the duration of this research journey. His invaluable mentorship, patience, and encouragement have been instrumental in shaping the development and completion of this thesis. I am truly grateful for Prof. Antoni Roig Batalla's dedication to excellence, his insightful feedback, and his willingness to share his knowledge and expertise. His mentorship has not only enriched my academic experience but has also inspired me to strive for excellence in my future endeavors.

In addition, I extend my heartfelt appreciation to all the professors who generously shared their knowledge and expertise throughout my research journey. Their dedication to teaching and guidance have played a crucial role in shaping my academic foundation. I am particularly grateful for their valuable recommendations, insightful feedback, and the wealth of knowledge they imparted during their courses.

Moreover, I am also grateful to the members of my thesis committee for their expertise, constructive feedback, and scholarly guidance.

Furthermore, I would like to acknowledge the Faculty of Law and staff for their support, resources, and opportunities that have enriched my academic experience.

Additionally, my heartfelt thanks go to my colleagues and peers for their camaraderie, encouragement, and intellectual exchange, which have been a source of inspiration and motivation.

Last but not least, I express my gratitude to the participants and contributors to my research, without whom this study would not have been possible. Particularly, I am indebted to my wife, Gülşah Tombul, and my parents, Leyla

Tombul and İsmail Hakkı Tombul, for their unwavering love, understanding, and encouragement, especially during the challenging moments of this journey. To all those who have played a part, whether big or small, in this journey towards the completion of my PhD, I extend my sincerest appreciation. Their support and encouragement have been invaluable, and I am deeply grateful for the privilege of undertaking this scholarly endeavor.

ABSTRACT

In light of recent global events, legislators and scholars within the legal domain find themselves compelled to reassess the safeguarding of personal data in the context of contact tracing applications. The advent of the first global pandemic in an era dominated by digital technologies has bestowed unprecedented surveillance capabilities upon governments during outbreaks. Although the subject may initially appear concise, it necessitates a comprehensive examination due to its multifaceted nature. Legal practitioners, academics, and governmental bodies have articulated their perspectives on this issue. While law firms, scholars, and public institutions have offered preliminary insights, a nuanced exploration directly tied to the research position is notably absent. The pandemic has underscored the potential necessity for global seclusion in response to future biological threats. The primary motivation behind such isolation is the protection of human health. In the contemporary digital age, an exhaustive investigation into the precautions to be taken and their implications for the protection of individuals' personal data becomes imperative. Amidst the paramount consideration of safeguarding the right to life for all members of society, it is equally crucial to ensure the protection of their right to privacy and personal data. While the precedence of the right to life is acknowledged, a comprehensive evaluation of all facets of the event, with particular emphasis on the protection of personal data, is imperative. Neglecting this aspect could potentially lead to profound challenges for humanity once the pandemic is surmounted. Consequently, this research endeavours to contribute substantively to the discourse on privacy-preserving requirements for contact tracing applications. It aims to achieve this by conducting an in-depth analysis of personal data protection, thereby enhancing data protection efficacy within the European Union, European Economic Area, and Spain. The primary objective of this study extends beyond addressing the data protection aspects of current contact tracing applications; it seeks to establish a robust data protection/privacy framework to address potential applications that may emerge in the future.

KEYWORDS: DIGITAL CONTACT TRACING, PANDEMIC, DATA PROTECTION

RESUMEN

A la luz de los recientes acontecimientos globales, los legisladores y académicos dentro del ámbito jurídico se ven obligados a reevaluar la protección de los datos personales en el contexto de las aplicaciones de rastreo de contactos. La llegada de la primera pandemia global en una era dominada por las tecnologías digitales ha otorgado capacidades de vigilancia sin precedentes a los gobiernos durante los brotes. Aunque el tema puede parecer inicialmente conciso, requiere un examen exhaustivo debido a su naturaleza multifacética. Profesionales del derecho, académicos y organismos gubernamentales han articulado sus perspectivas sobre esta cuestión. Aunque bufetes de abogados, académicos e instituciones públicas han ofrecido visiones preliminares, falta una exploración matizada directamente ligada a la posición de investigación. La pandemia ha subrayado la potencial necesidad de aislamiento global en respuesta a futuras amenazas biológicas. La motivación principal detrás de este aislamiento es la protección de la salud humana. En la era digital contemporánea, se hace imperativo llevar a cabo una investigación exhaustiva sobre las precauciones que se deben tomar y sus implicaciones para la protección de los datos personales de los individuos. En medio de la consideración primordial de salvaguardar el derecho a la vida para todos los miembros de la sociedad, es igualmente crucial asegurar la protección de su derecho a la privacidad y a los datos personales. Aunque se reconoce la precedencia del derecho a la vida, es imprescindible una evaluación exhaustiva de todos los aspectos del evento, con especial énfasis en la protección de los datos personales. Negligir este aspecto podría conducir a profundos desafíos para la humanidad una vez superada la pandemia. En consecuencia, esta investigación pretende contribuir sustantivamente al discurso sobre los requisitos de preservación de la privacidad para las aplicaciones de rastreo de contactos. Tiene como objetivo lograrlo mediante un análisis exhaustivo de la protección de los datos personales, mejorando así la eficacia de la protección de datos dentro de la Unión Europea, el Espacio Económico Europeo y España. El objetivo principal de este estudio va más allá de abordar los aspectos de protección de datos de las aplicaciones de rastreo de contactos actuales; pretende establecer un marco robusto de protección de datos y privacidad para abordar las posibles aplicaciones que puedan surgir en el futuro.

PALABRAS CLAVE: RASTREO DE CONTACTOS DIGITALES, PANDEMIA, PROTECCIÓN DE DATOS

RESUM

A la llum dels recents esdeveniments globals, els legisladors i acadèmics dins del camp jurídic es veuen obligats a reavaluar la protecció de les dades personals en el context de les aplicacions de rastreig de contactes. L'arribada de la primera pandèmia global en una era dominada per les tecnologies digitals ha atorgat capacitats de vigilància sense precedents als governs durant els brots. Tot i que el tema pot semblar inicialment concís, requereix un examen exhaustiu a causa de la seva naturalesa multifacètica. Professionals del dret, acadèmics i organismes governamentals han articulat les seves perspectives sobre aquesta qüestió. Tot i que bufets d'advocats, acadèmics i institucions públiques han ofert visions preliminars, manca una exploració matisada directament lligada a la posició de recerca. La pandèmia ha subratllat la potencial necessitat d'aïllament global en resposta a futures amenaces biològiques. La motivació principal darrere d'aquest aïllament és la protecció de la salut humana. En l'era digital contemporània, esdevé imperatiu dur a terme una investigació exhaustiva sobre les precaucions que s'han de prendre i les seves implicacions per a la protecció de les dades personals dels individus. Enmig de la consideració primordial de salvaguardar el dret a la vida per a tots els membres de la societat, és igualment crucial assegurar la protecció del seu dret a la privacitat i a les dades personals. Tot i que es reconeix la precedència del dret a la vida, és imprescindible una avaluació exhaustiva de tots els aspectes de l'esdeveniment, amb especial èmfasi en la protecció de les dades personals. Negligir aquest aspecte podria conduir a profunds desafiaments per a la humanitat un cop la pandèmia estigui superada. En conseqüència, aquesta investigació pretén contribuir substantivament al discurs sobre els requisits de preservació de la privacitat per a les aplicacions de rastreig de contactes. Té com a objectiu aconseguir-ho mitjançant una anàlisi exhaustiva de la protecció de les dades personals, millorant així l'eficàcia de la protecció de dades dins de la Unió Europea, l'Espai Econòmic Europeu i Espanya. L'objectiu principal d'aquest estudi va més enllà d'abordar els aspectes de protecció de dades de les aplicacions de rastreig de contactes actuals; pretén establir un marc robust de protecció de dades i privacitat per abordar les possibles aplicacions que puguin sorgir en el futur.

PARAULES CLAU: SEGUIMENT DIGITAL DE CONTACTES, PANDÈMIA, PROTECCIÓ DE DADES

INTRODUCTION

The Covid-19 pandemic and its effects on people's daily lives on a global scale and the situation of the healthcare system obliged countries to invent an efficient way to avoid thereto. This invention did not only take place in the healthcare system of the countries and medical measures, but also in digital solutions in line with the requirements of this era. In other words, each government endeavoured to support its healthcare system with efficient detection and surveillance system conducted through e-applications. Contact tracing, identifying individuals that have been in contact with an infected person, is a key component in tackling the spread of infectious illnesses.¹ To this end, contact tracing techniques have been in use for over five centuries to manage the spread of diseases like syphilis, initiated by a team of Italian doctors investigating the epidemic's origins to find the "patient zero".² Throughout medical history, instances like AIDS and Ebola have utilized tracing methods to identify symptomatic individuals and implement necessary isolation measures.³ A public health professional still conducts traditional contact tracing, which entails interviewing an infected individual to identify their contacts and advise those exposed to self-monitor for symptoms, self-quarantine, or seek medical evaluation and treatment.⁴ However, the traditional method is labor- and time-intensive, making it difficult to scale up as the number of COVID-19 infections increases, and, it is less effective due to COVID-19's shorter serial interval.⁵ Therefore, in this context, data flowing

¹ Anglemeyer Andrew; Moore, Theresa HM; Parker, Lisa; Chambers, Timothy; Grady, Alice; Kellia Chiu et al (2020) "Digital contact tracing technologies in epidemics: a rapid review", *Cochrane Database of Systematic Reviews*, Vol. 8, Issue 8, pp.1-44, p.4.

² Scantamburlo, Teresa; Cortés, Atia; Dewitte, Pierre; Van der Eycken, Daphné; De Wolf, Ralf and Martens, Marijn (2021) "Covid-19 and tracing methodologies: A lesson for the future society", *Health Technol.*, vol. 11, pp. 1051-1061, p.1052.

³ *Ibid.*

⁴ Kleinman, Robert A., and Merkel, Colin (2020) "Digital contact tracing for COVID-19", *Cmaj*, vol.192, no. 24, pp. E653-E656, p.e653.

⁵ *Ibid.*

from smartphones can help identify who, where, and how people get infected who might be at risk. Applications used on mobile phones displaying health data to third parties can be shown as an example here. While the World Health Organization and several countries were discovering what sort of innovations must have been introduced as a response to the outbreak,⁶ many technology companies, including Google, Apple, Microsoft⁷, Amazon and etc., worked on this issue to respond such need. For this reason, an application that warns when people are diagnosed with infection around the person has been developed by the joint efforts of these technology companies and governments. This innovation was then defined as digital contact tracing.

Contact tracing applications serve a multifaceted role beyond merely alerting individuals to potential virus exposure. They also play a crucial role in monitoring the quarantine process, tracking symptoms, and facilitating self-medical reporting. Symptom-tracking tools, for instance, primarily rely on the collection of self-reported signs and symptoms to gauge the prevalence of the epidemic and inform contact tracing efforts. This broader functionality underscores the integral role that contact tracing apps play in not only identifying potential transmission chains but also in supporting public health interventions aimed at containing the spread of infectious diseases. Therefore, contact tracing solutions are evaluated to be massively effective to take an action as preventive or control measures,⁸ and case studies, also, may be a valuable tool for locating additional contacts who are particularly at risk of contracting COVID-19.⁹ However, the rapid development and deployment of these applications have raised concerns about protection of personal data of the users. The fundamental reason is contact tracing

⁶ Anglemyer Andrew; Moore, Theresa HM; Parker, Lisa; Chambers, Timothy; Grady, Alice; Kellia Chiu et al. (2020) "Digital contact tracing...", *op. cit.*, p.4

⁷ See Covid Safe- Microsoft joint app <https://covidsafe.cs.washington.edu/> (accessed on 19 November 2022)

⁸ Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2021) "Effectiveness modelling of digital contact-tracing solutions for tackling the COVID-19 pandemic", *The Journal of Navigation*, vol.74, no. 4, pp.853-886, p.853

⁹ *Ibid.*

applications process sensitive information about individuals' health status, location, and contacts, which, if misused, could result in significant harm to the privacy of individuals. The privacy risks associated with contact tracing applications may include the unauthorized access and use of personal data, the risk of data breaches, and the exposure of sensitive information to third parties, and other potential data protection risks.

Correspondingly, this work undertakes a comprehensive review of data protection law aspects in both Spanish and other European contact tracing applications, i.e. the EU/EEA contact tracing applications, aiming to assess the associated risks with use of these applications, compliance activities of data controllers under applicable regulations and propose effective risk mitigation strategies to comply with data protection law necessities, in addition to their existing compliance efforts. By examining the data protection law related implications of these applications and evaluating their compliance with relevant data protection regulations and guidelines, this study seeks to provide insights into current privacy practices of data controllers and identify opportunities for improvement for their future use instead of simply ruling out the use of these applications due to its data protection law related risks. By conducting a thorough review of data protection aspects of different contact tracing platforms, we aim to identify common challenges and best practices in ensuring data privacy and security in the context of data protection law matters. Moreover, we will meticulously scrutinize the legal frameworks pertinent to data protection and contact tracing applications, encompassing relevant data protection regulations and laws, judicial precedents, decisions from data protection agencies, and best practices in data protection remit. Through this comprehensive approach, we endeavour to provide a nuanced understanding of the intricate interplay between data protection regulations as well as best practices and the deployment of contact tracing technologies in the digital landscape.

Building upon the findings of our review of the existing specific risks and compliance activities of controllers, this thesis will explore cutting-edge data privacy solutions within the form of technical and organizational measures to mitigate the identified risks associated with contact tracing applications. Drawing on insights from privacy-enhancing technologies (PETs) including

but not limited to cryptography, centralized and decentralized architectures, blockchain methods, smart contracts and many others, we will discover and propose innovative technical and organizational approaches to prioritize user privacy and autonomy without compromising the efficacy of contact tracing efforts. In the parallel vein, we will also propose more novel approaches for the existing approaches stipulated under the GDPR, such as encryption, pseudonymization, anonymization and so on, to enable collaborative data analysis while minimizing the disclosure of sensitive information. By integrating these advanced privacy-enhancing measures into contact tracing applications, we aim to strike a balance between public health objectives and individual privacy rights, fostering trust and acceptance of these contact tracing technologies among diverse user groups, rather than simply rejecting the use of applications due to their privacy side-effects.

Hence, in other words, we are aiming to explore how future applications to be used within the scope of contact tracing activities can better mitigate data protection risks, thereby complying with data protection law requirements more successfully. By evaluating current privacy practices, identifying regulatory challenges, and proposing innovative solutions, we seek to contribute to the ongoing discourse on the responsible use of technology in public health surveillance implemented by controllers and inform policy discussions of regulators/data supervisory authorities aimed at protecting individual privacy rights during the use of contact tracing activities to find a response on the question, namely if privacy-friendly contact tracing applications are possible or not. Considering that contact tracing applications become more widespread and critical in controlling the spread of infectious diseases, it is essential to understand the implications for data protection and to develop measures to ensure that these applications are used in a way that is consistent with data protection, as it might be used by countries again for the future pandemic scenarios. That being said, each country shapes their contact tracing applications according to the characteristics of the institution and society. In some countries, the acquisition of these applications is mandatory for almost all citizens. For instance, authorities in Asia, where the virus first emerged, many governments did not request permission from individuals before tracking their cell phones to identify suspected coronavirus

patients.¹⁰ Accordingly, South Korea, China, and Taiwan, after initial outbreaks, reached early successes in reducing the cases through their use of tracking programs. Or similarly, Thailand was giving all new arrivals at its airports a free SIM card and asking them to download an application that tracked their location for 14 days.¹¹ On the other hand, some countries, particularly the EEA/EU countries (hereinafter they will be cumulatively called as “European Countries” or as the EEA/EU countries or EEA countries), i.e. the GDPR jurisdictions¹², did not oblige their citizens/residents to download these applications but rather demand to use them effectively. Accordingly, to narrow down the scope of the research due to jurisdictional differences across the regions, we will merely deal with the European and more specially Spanish aspects of data protection matters within the scope of the digital contact tracing activities. The reason is that discussing the data protection aspects of each country in the World, with respect to the application of contact tracing applications, would be excessively time-consuming and fruitless, as every jurisdiction and country has its own characteristics, and it is therefore unrealistic to generate a “one-for-all” solution. Thus, the focus of the compliance assessment of the applications are limited to the European and Spanish Data Protection framework for contact tracing applications, i.e.,

¹⁰ See The Wall Street Journal article, South Korea Tracks Virus patients travels and publishes them online available at: https://www.wsj.com/articles/south-korea-tracks-virus-patients-travels-and-publishes-them-online11581858000?mod=searchresults&page=1&pos=2&mod=article_online (accessed on 19 November 2022)

¹¹ See Privacy International, Thailand: Sim Card and App to track travellers <https://privacyinternational.org/examples/3452/thailand-sim-card-and-app-track-travellers> (accessed on 10 January 2021)

¹² The GDPR is also applicable in the EEA states, in addition to the EU, by virtue of Decision No. 154/2018 of the EEA Joint Committee. For further information see Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022] (OJ L 183 19.07.2018, p. 23, ELI: <http://data.europa.eu/eli/dec/2018/1022/oj>)

GDPR¹³, Ley Orgánica 3/2018 (LOPDyGDD)¹⁴, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020¹⁵, e-Privacy Directive¹⁶, EU Toolbox¹⁷, Recommendation on Apps¹⁸, Spanish Constitution¹⁹, Spanish Healthcare Laws and relevant Orders, and AEPD guidelines and their implementation in Spain.

Overall, we are aiming to contribute to the existing literature on data protection and digital contact tracing applications by scrutinizing the inherent risks posed by these technologies, evaluating data controllers' compliance with regulatory frameworks, and proposing further cutting-edge risk mitigation and compliance strategies, thereby contributing to the development of robust privacy safeguards that reconcile the dual objectives of effective pandemic surveillance and privacy preservation in their potential future use again, considering that we live in era of technology and unfortunate infections disease, which may oblige governments to opt for this technology again in the future. As such, through a comprehensive analysis, this thesis seeks to foster

¹³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter referred as 'GDPR').

¹⁴ Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD).

¹⁵ EDPB (2020) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020

¹⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (the "ePrivacy Directive")

¹⁷ Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, published on 15 April 2020

¹⁸ Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

¹⁹ Spanish Constitution Passed by the Cortes Generales in Plenary Meetings of the Congress of Deputies and the Senate held on October 31, 1978 Ratified by the spanish people in the referendum of December 6, 1978 Sanctioned by His Majesty the King before the Cortes on December 27, 1978

a deeper understanding of the legal, and technological dimensions of contact tracing privacy, paving the way for the responsible and privacy friendly deployment of digital health interventions in a rapidly evolving digital landscape and find a response for the most privacy friendly contact tracing approach in the GDPR jurisdiction for their future use. Although many academic articles were published regarding the fundamental data protection concerns related to the topic, they did not really address each specific feature of the data protection attitude of data controllers from holistic point of view with sufficient details. Therefore, the results of this research are not only targeting to support data controllers (owners) of the applications, but also other actors involved in the process, such as data protection authorities/regulators for any potential future use of contact tracing applications for another infectious disease in the future.

In addition to the overarching research question delineated above, our inquiry delves into various granular aspects at the nexus of data protection laws and contact tracing applications to have the full visibility on the data protection aspects of contact tracing activities. For instance, this thesis will dive into the specific privacy considerations of contact tracing apps, as it is essential to recognize the inherent risks associated with their widespread use. The extensive collection of personal data, including location information, health status, and social interactions, raises concerns regarding unauthorized access, misuse, or data breaches, potentially exposing individuals to various forms of harm such as identity theft or targeted advertising. Accordingly, we scrutinize the involvement of third-party technology companies such as Google or Apple (GAEN)²⁰, Amazon²¹ or Microsoft²² etc., whose integration with contact tracing applications has raised societal concerns regarding data

²⁰ See Apple, Apple and Google partner on Covid-19 contract tracing technology <https://www.apple.com/pl/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> (accessed on 23 June 2024)

²¹ See Amazon, Covid-19 Contact Tracing Platform <https://aws.amazon.com/marketplace/pp/prodview-gsckcplivo452> (accessed on 23 June 2024)

²² See Covid Safe- Microsoft joint app <https://covidsafe.cs.washington.edu/> (accessed on 23 June 2024)

amalgamation across different platforms. Furthermore, we will meticulously analyse potential contact tracing specific risk areas, including intrusive location tracking, re-identification of data subjects, and over-retention of personal data, while concurrently offering pragmatic solutions from a data protection law perspective. In other words, we will also probe the most pertinent technology and data security risks arising from the involvement of multiple parties and applications, such as the re-identification of data subjects. Thus, all these concerns and ambiguous aspects will be investigated and addressed in detail in the related chapters.

Similarly, we will delve into the potential legal and regulatory ramifications stemming from the architectural and processing methodology choices of the applications, considering that the EDPB recommended the adoption of both centralized and decentralized systems provided that adequate security measures are implemented.²³ For instance, countries such as France or Norway prefer centralized data processing.²⁴ On the contrary, the UK government, a former EU member using the UK GDPR, declared that the UK was leaving a centralized NHS contact-tracing app for England and changing to a decentralized version, based on the GAEN toolkit.²⁵ As such, our discourse aims to elucidate the implications of these choices within the purview of data protection laws, contextualized by the latest technological and legal developments.

Likewise, from a risk-based perspective, our analysis will encompass an evaluation of purpose limitation²⁶, data minimization²⁷ practices, retention

²³ See EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9

²⁴ See European Commission Website, Mobile Contact Tracing Apps in EU https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (accessed on 23 June 2024)

²⁵ See BBC Website, Technology <https://www.bbc.com/news/technology-52441428> (accessed on 10 July 2022)

²⁶ Article 5-1-b of the GDPR, purpose limitation.

²⁷ Article 5-1-c of the GDPR, data minimization.

periods²⁸, lawful basis of processing²⁹, data subjects' rights³⁰, data protection/privacy by design and default³¹, security of processing³², data protection impact assessments³³ and other key aspects of the data protection compliance activities of the controllers in light of the legal framework. Our objective is to furnish tailored recommendations for data controllers, informed by a nuanced understanding of these measures. To facilitate this, we pose critical questions regarding the fate of processed data and the implementation of these principles from controllers' perspective. In a parallel vein, the second part of this thesis scrutinizes technical and organizational measures under the European regime, alongside matters of data privacy-by-design and default practices, considering that these topics, sensitive and intricate, necessitate meticulous examination and are accompanied by concrete recommendations in light of the latest technological advancements.³⁴ Hence, in this section of the thesis, we will provide our most remarkable contribution to the literature as our thesis question is targeting to provide most cutting-edge solutions for more efficient compliance with data protection law necessities, while at the same time tackling the risks to be detailed. Accordingly, we contemplate the utilization of novel technologies from diverse realms of data protection literature to mitigate these concerns, evaluating the efficacy of measures under the GDPR and collaboration with European agencies for the deployment of state-of-the-art data security solutions. Thus, in summary, these inquiries, alongside all other emergent topics, undergo thorough legal

²⁸ Article 5-1-e of the GDPR, storage limitation.

²⁹ Article 6 of the GDPR, lawfulness of processing

³⁰ Articles 12 to 23 of the GDPR, rights of the data subject.

³¹ Article 25 of the GDPR, data protection by design and by default

³² Article 32 of the GDPR, security of processing

³³ Article 35 of the GDPR, data protection impact assessment

³⁴ Pierucci, Alessandra, Jean-Philippe Walter, and Data Protection Commissioner (2020) "Joint statement on digital contact tracing." Council of Europe. https://epic.org/wp-content/uploads/privacy/covid/Covid19_joint_statement.pdf (accessed on 26 May 2024), p.6

analysis and are addressed through the integration of innovative technological approaches across the chapters of this research.

As for the limitation on the scope of this research, we would like to state that while this research provides a comprehensive analysis of the data protection aspects of contact tracing applications, it is important to note that it does not delve into the efficacy or effectiveness of these applications in mitigating the spread of infectious diseases. The focus of this study is primarily on examining the compliance of these applications with data protection regulations, identifying privacy risks, and proposing mitigation strategies. Hence, the broader functionality and impact of contact tracing applications in public health surveillance are beyond the scope of this research.

Regarding the structure of the research, in the first part of the thesis, Chapter 1 will lay the groundwork by introducing the general features of contact tracing applications, including their fundamental technical aspects and pertinent privacy policies where applicable. This introductory phase aims to provide a general understanding of the key components and functionalities of these applications, drawing upon real-life examples from various countries, including but not limited to our jurisdictional focus (EEA), to enrich the discussion.

Subsequently, Chapter 2 will delve into a detailed delineation of the novel data protection risks inherent in the use of contact tracing applications. Through the presentation of specific real-life examples, this section will offer an in-depth analysis of the prevailing landscape. In addition to addressing generic risks, which are already significant and called out in the literature, this chapter will explore contact-tracing specific emerging risk categories and users' perceptions and concerns regarding the use of contact tracing applications.

Moving on to the second part of the thesis, Chapters 3, 4, and 5 will delve into a detailed examination of the actions undertaken by data controllers vis-à-vis European data protection standards. Following an assessment of the nexus between the prevailing legal landscape in the EU and EEA, and the operational dynamics of contact tracing applications, we will proceed to present our bespoke recommendations and solutions tailored to assist data controllers in achieving compliance with existing European data protection

standards. The most striking aspect of our thesis for the European applications will manifest in these chapters, where innovative and cutting-edge solutions will be proposed to address the intricate challenges posed by data protection laws and the deployment of contact tracing applications.

In more detail, within Chapters 3 and 4, we will delineate best practices aimed at facilitating transparent information dissemination, lawful basis of processing activities, data minimization, purpose limitation, privacy-by-design and default, security of processing and data protection impact assessments—crucial requirements incumbent upon data controllers under prevailing European regulations. This entails exploring innovative methodologies, as briefly introduced above, such as the integration of blockchain technology, to mitigate risks associated with data minimization and re-identification of personal data processed by applications, aligning with pertinent regulations and guidelines. The overarching objective of these chapters is to ensure the effective protection of the rights and freedoms of data subjects domiciled in Europe, thereby underscoring the central theme of this in-depth analysis and recommendations.

Furthermore, Chapter 5 will not only assess the extent of adherence to existing guidelines by data controllers but will also scrutinize potential areas for improvement from the perspectives of both controllers and regulators within the framework of European data protection guidelines on contact tracing applications to provide more holistic approach for privacy-friendly applications. In other words, in this Chapter, we will also provide tailor-made recommendations for regulators and controllers for the future utilization of these applications in the EEA from a data protection law perspective.

On the back of these analyses on the European level, in the third part of the research, namely in Chapter 6, the issues that were not widely mentioned in the existing Spanish data protection and pandemic literature is going to be

addressed i.e., the role of guidelines of AEPD³⁵, the exceptional Regulation³⁶, interpretation of constitutional court decision³⁷, other relevant orders as well as Health Regulations and the GDPR in conjunction with Ley Orgánica 3/2018³⁸ will be investigated. In addition, the legal framework of pandemic management in Spain, implementation of data protection requirements under the pandemic conditions, and requirement for a new healthcare law will be discussed and analysed as well, which will also create the basis of the discussions for Spanish digital contact tracing activities from regulators perspective.

In the last chapter, namely Chapter 7, an analysis on the current status of contact tracing applications will be conducted. Furthermore, the root cause of potential data protection law failures for Spanish system both from technical and implementational perspective, and the lessons learned from the current situation for the future case scenarios in Spain, by analysing compliance of data controllers under the GDPR³⁹ and LOPDyGDD⁴⁰, as well as respective AEPD guidelines, scholar's view and AEPD decisions on Radar Covid application will be delivered. Finally, in the last subchapter of Chapter 7, after analysing all these issues and providing ideas on efficient compliance mechanisms both in EEA and Spain respectively through the chapters of this research, our conclusive remarks summarizing our thesis statement and scientific contributions to the literature of contact tracing activities are going to be provided.

³⁵ For further information see the website of Agencia Española de Protección de Datos <https://www.aepd.es/en/areas/data-protection-and-covid-19> (accessed on 5 February 2023)

³⁶ Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19

³⁷ Tribunal Constitucional de España, Sentencia 148/2021, de 14 de julio (BOE Núm. 182, de 31 de Julio De 2021), Ecli:Es:Tc:2021:148.

³⁸ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

³⁹ Article 24 of the GDPR, responsibility of data controllers.

⁴⁰ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

The methodologies will be used in this research to obtain results are as follows:

- Review of privacy policies of contact tracing applications in the EEA/EU: Understanding the privacy policies of contact tracing apps within the European Economic Area /European Union is crucial for assessing how user data is collected, stored, and processed. This analysis will also support us in evaluating the level of transparency and adherence to data protection regulations, providing insights into potential privacy risks and legal compliance.
- Review of terms and conditions documents, and where available, technical specifications of contact tracing applications EEA/EU: Examining the available terms and conditions documents along with technical specifications of contact tracing apps is essential to comprehend the rights and obligations of users, as well as the technical mechanisms involved in data collection and processing. This review will also assist us in understanding details of data processing activities and identifying potential privacy vulnerabilities and assessing the adequacy of technical safeguards.
- Review of data protection/privacy literature on global scale and comparative analysis thereof: Conducting a comprehensive review of data protection and privacy literature globally will allow for a broader understanding of emerging trends, best practices, and challenges in the context of data protection law field. Comparative analysis will also enable the identification of commonalities and differences in regulatory approaches across jurisdictions, informing recommendations for effective data protection measures.
- Review of digital contact tracing activities literature and their data protection implications on global scale: Reviewing literature on

digital contact tracing activities globally provides insights into various strategies employed for disease surveillance and their respective data protection implications. This review aids in contextualizing digital contact tracing and assessing its privacy implications.

- Review and interpretation of the existing case law in data protection law field: Interpreting existing case law in the field of data protection law helps in understanding judicial interpretations of relevant legal principles and precedents. This review assists in predicting potential legal outcomes and guiding legal arguments regarding data protection issues arising from digital contact tracing applications.
- Review and interpretation of decisions of the European Data Protection Board, European Data Protection Supervisor, European Commission and Local Data Protection Authorities of the Member States: Examining decisions of key data protection authorities at both European and national levels provides insights into their enforcement practices and interpretations of data protection laws concerning digital contact tracing. This review feeds compliance strategies and risk mitigation measures for developers and operators of contact tracing apps.
- Review and interpretation of the Guidelines of European Data Protection Board, European Data Protection Supervisor, European Commission, European Parliament and further European Institutions and Local Data Protection Authorities of the Member States.: Studying guidelines issued by relevant European institutions and local data protection authorities will offer practical guidance on complying with data protection requirements in the development and deployment of contact tracing applications. This review assists stakeholders in aligning their practices with regulatory expectations and promoting user privacy.
- Review and interpretation of the former decisions of Court of Justice of the European Union within the data protection law remit:

Analysing previous decisions of the Court of Justice of the European Union (CJEU) in the field of data protection law provides insights into legal interpretations and principles relevant to digital contact tracing. This review informs the legal analysis and strategic decision-making process concerning data protection compliance and risk management.

- Review and interpretation of the sources of AEPD and other public institutions in Spain within respect the data protection law and pandemic: Interpreting sources from the Spanish Data Protection Agency (AEPD) and other public institutions in Spain regarding data protection law and pandemic response offers insights into national regulatory frameworks and enforcement priorities. This review aids in understanding the specific legal and regulatory context within Spain and informing compliance efforts accordingly.
- Review and interpretation of the decisions of Courts in Spain and AEPD: Interpreting decisions of courts in Spain and the AEPD will provide us with specific insights into legal interpretations and enforcement actions related to data protection issues arising from digital contact tracing within the Spanish jurisdiction. This review informs compliance strategies and risk mitigation measures tailored to the Spanish legal context.
- Review and interpretation of data protection and healthcare relevant Spanish legislation: Analysing relevant data protection and healthcare legislation in Spain will help us in our understanding the legal requirements and obligations applicable to the development and operation of contact tracing applications in the Spanish context. We will interpret the data protection implications of these laws within the scope of digital contact tracing activities.

PART I

CONTACT TRACING APPLICATIONS AND THEIR POTENTIAL THREAT TO DATA PROTECTION

I. THE MAIN FEATURES OF CONTACT TRACING APPLICATIONS

1. General Framework

1.1 Purpose

Contact tracing, along with comprehensive testing, isolating cases, and providing proper care, stands as a crucial strategy in breaking the chains of SARS-CoV-2 transmission and reducing the mortality linked to Covid-19.⁴¹, as described in the introduction part. Correspondingly, the fundamental objective of contact tracing is to interrupt the transmission of a disease by promptly notifying individuals who have been in close proximity to an infected person, apprising them of their heightened risk, and imparting guidance on preventive measures to curtail further dissemination.⁴² Having said that, digital proximity tracking does not merely rely on the technical functioning of the proximity tracing application and its backend server, but also on seamless integration of health system processes i.e., laboratory testing, communication of results, generation of notification codes, manual contact tracing, and management of application notified users.⁴³ Therefore, we are of view that in order to investigate the data protection aspects and implications of these applications, there is a requirement to be aware of the fundamentals of these applications. Accordingly, further following information is going to illuminate the general features and components of the applications, their types, use cases in

⁴¹ World Health Organization, (2021) "Contact tracing in the context of COVID-19, interim guidance", available at: https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y (accessed on 23 June 2024), p1.

⁴² See European Centre for Disease Prevention and Control (2020), "Mobile applications in support of contact tracing for COVID-19 – A guidance for EU/EEA Member States," 10 June 2020. Stockholm: ECDC, available at: <https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing>, (accessed on 23 June 2024).p.2.

⁴³ Lueks, Wouter; Benzler, Justus; Bogdanov, Dan; Kirchner, Göran; Lucas, Raquel; Oliveira, Rui; Preneel, Bart; Salathé, Marcel; Troncoso, Carmela and von Wyl, Viktor. (2021) "Toward a common performance and effectiveness terminology for digital proximity tracing applications", *Frontiers in digital health*, vol.3, 677929, pp.1-12, p.2.

different countries, main difference from other digital tools, methods of processing personal data and other required details, which will act as an introductory information prior to the in-depth legal analysis through the following chapters of this thesis.

1.2 Classification of digital applications used in COVID-19

There were typically variety of applications with different purposes used during the pandemic days. Hence, prior to delving into the nuances of contact tracing applications, we are of view that it would be fruitful to distinguish between other digital applications and contact tracing applications, both of which were utilized during the pandemic. The reason being is that the term of “application” seems to be open to the confusion in the eyes of individuals, due to both of their unique nature. Therefore, to begin with the other applications utilized during the pandemic, we can simply list self-diagnosis and quarantine enforcement applications. For instance, regarding the self-diagnosis tracing applications that have been released in Western nations predominantly focus on self-diagnosis, symptom tracking, and informing health authorities of instances.⁴⁴ To be more specific, symptom checker applications are mobile or online tools that enable non-medical individuals to identify potential reasons for their symptoms and offer advice on whether they should seek medical attention.⁴⁵ As such, a webpage or mobile phone app with COVID-19 compatible question and answer capability is referred to as having symptom checker capabilities.⁴⁶ The most remarkable aspect of these applications are

⁴⁴ See, Margherita Russo, Claudia Cardinale Ciccotti, Fabrizio De Alexandris, Antonela Gjinaj, Giovanni Romaniello, Antonio Scatorchia, Giorgio Terranova (2021) CEPR VOXEU Website Article available at: <https://voxeu.org/article/cross-country-comparison-contact-tracing-apps> (accessed on 19 November 2022).

⁴⁵ Müller, Regina, Malte Klemmt, Roland Koch, Hans-Jörg Ehni, Tanja Henking, Elisabeth Langmann, Urban Wiesing, and Robert Ranisch. (2024) “That’s just Future Medicine”-a qualitative study on users’ experiences of symptom checker apps”, *BMC Medical Ethics*, vol. 25, no. 1, pp.17-36, p.17.

⁴⁶ See eHealth Network (2020) Mobile applications to support contact tracing in the EU’s fight against COVID-19 Common EU Toolbox for Member States available at: https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf, (accessed on 23 June 2024), p.44

the ability of making recommendations on whether testing is needed and how to reduce the risk of infecting others.⁴⁷ Therefore, these applications' symptom checker feature also helps countries supplement primary care monitoring and learn more about COVID-19 in their communities.⁴⁸ This data has been compiled with data from more extensive testing of symptomatic people as part of the COVID-19 surveillance system.⁴⁹ For instance, AsistenciaCovid19, which began as a trial in the Community of Madrid and has been adopted by other autonomous regions in Spain,⁵⁰ included a questionnaire that allows users to determine whether their symptoms are consistent with COVID-19 symptoms. The application then made suggestions about whether to isolate or call health care based on this data⁵¹. It also enabled users to follow the progression of their symptoms.⁵² Users could also choose to share their device's location data with the application, which they claim on the application's website is "for the goal of ensuring the data quality and its epidemiological analysis".

Likewise, some of the digital applications were also used for enforcing the quarantine by health or public authorities. As an illustration, these applications uphold quarantine measures by utilizing mobile phone signals and GPS

⁴⁷ See eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States available at: https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf, (accessed on 23 June 2024), p.44.

⁴⁸ *Ibid.*, p.44.

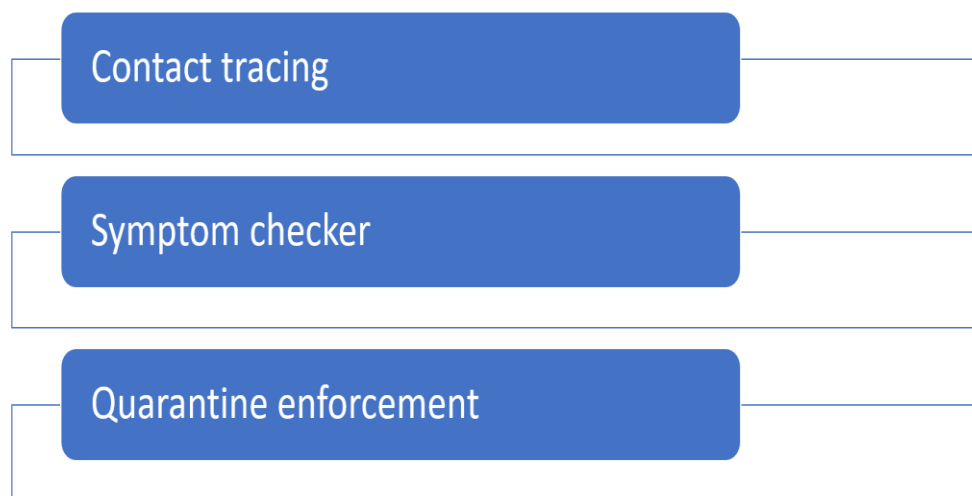
⁴⁹ *Ibid.*, p.44.

⁵⁰ See Resolución de 8 de mayo de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Comunidad Autónoma de Castilla-La Mancha, sobre la adhesión al uso de la Aplicación AsistenciaCOVID19., («BOE» núm. 150, de 27 de mayo de 2020, páginas 35080 a 35099 (20 págs.)), section "Objeto del Convenio".

⁵¹ See BBVA, (2020) How do Covid-19 tracing apps work and what kind of data do they use, available at: <https://www.bbva.com/en/how-do-covid-19-tracing-apps-work-and-what-kind-of-data-do-they-use/> (accessed on 15 August 2022).

⁵² *Ibid.*

technology to monitor user movements.⁵³ The idea is to establish a digital perimeter around individuals' residences.⁵⁴ Consequently, if they violate the regulations by leaving their homes, authorities are alerted. For instance, those cases are typically instructed to self-quarantine at home for fourteen days following their last exposure to the case, retain six feet of "social distancing" from other people during the "quarantine period," and self-monitor for signs, such as taking their temperatures a couple of times a day.⁵⁵



Nonetheless, as reiterated in the introduction that this thesis will focus on the contact tracing applications used within the EEA region. Therefore, symptom checker and self-diagnosis applications will only be referenced, if and when required for the analyse of contact tracing applications. Hence, after the brief clarification on the term of digital applications we would like to return to the main focus of the thesis, namely contact tracing applications. Accordingly, the tasks conducted by contact tracing applications could be accumulated into

⁵³ Singh, Hanson John Leon; Couch, Danielle and Yap, Kevin (2020) "Mobile health apps that help with COVID-19 management: scoping review." *JMIR nursing* 3, no. 1, e20596, pp.1-16, p.7.

⁵⁴ Singh, Hanson John Leon; Couch, Danielle and Yap, Kevin (2020) "Mobile health apps that help with COVID-19 management...", op.cit., p.7.

⁵⁵ See Trotogott, R. L. (2020) "A comparative analysis of data privacy impacted by COVID-19 contact tracing in the European Union, the United States, and Israel: sacrificing civil liberties for a public health emergency", *ILSA J. Int'l & Comp. L.*, vol.27, pp.55-76, p.57.

three groups, namely detection of contact events (proximity tests), transmission, and exposure notification.⁵⁶ This includes identifying those who are at risk based on their proximity to and on the length of contact with an infected individual or based upon environmental transmission.⁵⁷ Therefore, it is fair to state that contact tracing tools gauge the physical closeness between users in order to monitor their interactions.⁵⁸ This method, which may also involve patient reports or other non-digital means, helps to determine when users have been in contact with someone who has tested positive for the severe acute respiratory syndrome coronavirus.⁵⁹ Correspondingly, during the following subsections of this chapter, we will dive into aforementioned nuances of contact tracing applications to build the basis for our in-depth analysis of the applications.

1.3 Use cases across the World regarding their implementation of the applications

In order to analyse the features of European contact tracing applications thoroughly, we believe that it is crucial for our research to learn more about the way other countries operate their contact tracing applications, considering that, more than seventy-eight countries across the World developed digital contact tracing apps to limit the spread of the coronavirus.⁶⁰

⁵⁶ Nobre, Jéferson Campos; Rodrigues Soares, Laura; Roman Huaytalla, Brigette Olenka; da Silva Júnior, Elvandi and Zambenedetti Granville, Lisandro (2021) "On the Privacy of National Contact Tracing COVID-19 Applications: The Coronavirus-SUS Case", *arXiv preprint arXiv:2108.00921*, pp.1-7, p.1.

⁵⁷ See eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf, (accessed on 23 June 2024), p.40.

⁵⁸ Gasser, Urs; Ienca, Marcello; Scheibner, James; Sleight, Joanna and Vayena, Effy (2020) "Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid", *The Lancet Digital Health*, vol. 2, no. 8, pp. e425-e434, p.e426.

⁵⁹ *Ibid.*

⁶⁰ Scrivano, Noemi; Gulino, Rosario Alfio and Giansanti, Daniele (2022) "Digital Contact Tracing and COVID-19: Design, Deployment, and Current Use in Italy", *Healthcare* 2022, vol. 10, 67, <https://doi.org/10.3390/healthcare10010067>, pp.1-11, p.2.

Therefore, to begin with the real-life examples of the applications utilized in different regions and jurisdictions, following the outbreak of the COVID-19 crisis, China set up a national telecom data analysis platform managed by the Ministry of Information Industry Technology.⁶¹ This platform enabled telecom providers (China Mobile, China Unicom, and China Telecom) to offer tracking records of cell phone users' locations for the past 15 to 30 days.⁶² In addition to those, in China, Alipay and WeChat mobile applications were the primary sources of contact tracing. These applications assigned green, yellow, and red hues based on the user's self-reported data, travel history, health status, and government records.⁶³ The colour indicated whether the user is healthy (green), has been diagnosed with COVID-19 (yellow), or is a confirmed COVID-19 patient (red).⁶⁴ According to the Personal Data Security Specifications, personal data collected and used for public security purposes did not require the consent of the individuals providing it.⁶⁵

Subsequently, in Singapore, TraceTogether was the first centralized Bluetooth-based solution.⁶⁶ The application used Bluetooth data to determine who else is in close vicinity to the user.⁶⁷ The location permission was solely used to find the distance between users. For communication with neighbouring devices, each device created a random unique identifier on a

⁶¹ Norton Rose Fulbright, (2021) Contact Tracing Apps: new world for Privacy, China section available at: <https://www.nortonrosefulbright.com/en-cn/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy#China> (accessed on 18 May 2024).

⁶² Norton Rose Fulbright, (2021) Contact Tracing Apps: new world for Privacy, China section

⁶³ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines for contact tracing applications", arXiv preprint *arXiv:2004.13328*, <https://arxiv.org/pdf/2004.13328>, pp.1-10, p.3.

⁶⁴ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p. 3.

⁶⁵ Norton Rose Fulbright, (2021) Contact Tracing Apps: new world for Privacy, China section

⁶⁶ Vaudenay, Serge (2020) "Centralized or decentralized? The contact tracing dilemma", *Cryptology ePrint Archive*, pp. 1-31, p.29.

⁶⁷ *Ibid.*

regular basis.⁶⁸ In case a user became infected with COVID-19, they had to send their logged data to the government, which subsequently distributed it to other users for match. The government only knew the phone numbers of the registered users. Hence, no identifiable information was transmitted between the devices, and the government only had access to the phone numbers of the registered users. In the meantime, in South Korea, an extensive electronic surveillance system was used. More specifically, GPS-enabled location tracking, closed-circuit television recordings, and credit card transactions were used to aid contact tracing.⁶⁹ South Korea's application helped people to identify "places" where infected individuals have been in the past two weeks and alert users if they are within 100 meters of these locations.⁷⁰ This location information was gathered by the Korea Disease Control and Prevention Agency (Korea CDA) using smartphone GPS systems, CCTV, and in-person interviews. Interestingly, South Korea's apps did not use any personal information directly transmitted from the smartphones of infected individuals.⁷¹

Within the similar vein, the Government of India (GoI) announced the launch of its 'Aarogya Setu' contact tracing software.⁷² For registration, the application simply requested a phone number, but it also collected personal data of the users such as name, age, gender, occupation, and countries

⁶⁸ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p. 4.

⁶⁹ O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; Johnson, Kevin; Laffey, John; McNicholas, Bairbre; Nuseibeh, Bashar; O'Callaghan, Michael; O'Keeffe, Ian; Razzaq Aabdul; Rekanar, Kaavya; Richardson, Ita; Simpkin, Andrew; Storni, Cristiano; Tsvyatkova, Damyanka; Walsh, Jane; Welsh, Thomas and O'Keeffe, Derek (2021) "Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature", *JMIR Mhealth Uhealth*, vol. 9, n.6, e27753, pp. 1-23, p.2.

⁷⁰ Kim, Hwang (2021) "COVID-19 apps as a digital intervention policy: a longitudinal panel data analysis in South Korea." *Health Policy*, vol.125, no. 11, pp.1430-1440, p.1431.

⁷¹ Kim, Hwang (2021) "COVID-19 apps as a digital intervention policy:" *op.cit.* p.1431.

⁷² Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p. 4.

visited in the previous 30 days.⁷³ For tracing all contacts in the proximity of a Covid patient in the last 14 days, a unique identification number is generated using the phone number. According to the government, all recorded data has been stored locally and would be uploaded to a government server for further analysis. However, it has been unclear if the analytics would be performed on raw data and the findings anonymized, or whether the analytics were to be performed directly on an anonymised dataset. A user could also remove her account, but the data would be kept by Gol for 30 days before being erased.⁷⁴

Differently, in Brazil, the users of Coronavírus-SUS were informed about the application's privacy policy when first downloading it or after upgrading to the contact tracing version.⁷⁵ That policy set forth that no personal data was collected, no GPS data was used, all communications were encrypted, and all information was stored in data servers in Brazil, thereby there was no aim of finding out one's identity or the identity of whoever comes in contact with it.⁷⁶ Also, it was possible to use other features of the application, namely news and health facility map, and decline to use the contact tracing feature, but the user had to agree with the privacy policy to use these features as well.

In Japan, a health management application called Health Diary was developed by Health Tech Research Institute.⁷⁷ It allowed each person to register and manage the check items when a new coronavirus infection was suspected.⁷⁸ Data has been managed only on the smartphone and it would not be sent to the outside including our company unless the person himself

⁷³ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p.4.

⁷⁴ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p.4.

⁷⁵ Nobre, Jéferson Campos; Rodrigues Soares, Laura; Roman Huaytalla, Briggette Olenka; da Silva Júnior, Elvandi and Zambenedetti Granville, Lisandro (2021) "On the Privacy....", *op. cit.*, p.1.

⁷⁶ *Ibid.*

⁷⁷ Ocheja, Patrick; Cao, Yang; Ding, Shiyao and Yoshikawa, Masatoshi (2020) "Quantifying the Privacy-Utility Trade-offs in COVID-19 Contact Tracing Apps", *arXiv preprint arXiv:2012.13061*, pp.1-14, p.6.

⁷⁸ *Ibid.*

sends it to the outside based on his intention. There was also COCOA application in place used by Japanese government. Once COCOA is installed on a mobile phone, it used a Bluetooth sensor to detect and record the app IDs of other users who stay within 1 meter for more than fifteen minutes, even when the app is turned off.⁷⁹ Once a user was confirmed to be infected with COVID-19 and reports it through the app, those who were in close contact with them in the past fourteen days received a warning message.⁸⁰

Meanwhile, the UAE introduced three contact tracing apps. In more detail, the Abu Dhabi Department of Health initially launched StayHome, followed by TraceCovid. Most recently, the UAE introduced another tracing app called ALHOSN.⁸¹ These apps were designed to identify individuals who had been in close contact with infected persons, enabling authorities to promptly reach out and provide necessary healthcare treatments.⁸² The last app, ALHOSN, also included additional features, such as access to users' test results and a health color-coding system that indicates users' health status. According to publicly available information, ALHOSN was jointly launched by the Ministry of Health and Prevention, the Abu Dhabi Health Authority, and the Dubai Health Authority. It served as the official digital tracing app for the pandemic, integrating the features of the previous apps, namely StayHome and TraceCovid. The Government did not disclose plenty of details about the measures and actions taken to ensure data privacy, yet the Department of Health Abu Dhabi only stated that the privacy of personal information would be protected.⁸³

⁷⁹ Shoji, Masahiro; Cato, Susumu; Ito, Asei; Iida, Takashi; Ishida, Kenji; Katsumata, Hiroto and McElwain, Kenneth Mori (2022) "Mobile health technology as a solution to self-control problems: The behavioral impact of COVID-19 contact tracing apps in Japan", *Social Science & Medicine*, vol.306, p.115142.

⁸⁰ Shoji, Masahiro; Cato, Susumu; Ito, Asei; Iida, Takashi; Ishida, Kenji; Katsumata, Hiroto and McElwain, Kenneth Mori (2022) "Mobile health technology as a solution...." *op.cit.*, p.115142.

⁸¹ Norton Rose Fulbright, (2021) Contact Tracing Apps: new world for Privacy, UAE section

⁸² *Ibid.*

⁸³ *Ibid.*

Lastly, in the USA, there had been a bunch of new contact tracing apps released at the time. In a decentralized arrangement, the 'Covid Watch' and 'CoEpi' apps utilized Bluetooth for proximity-based contact tracing.⁸⁴ Both of these apps assessed signal strength in order to determine the distance between users. In case the user stayed in contact for a certain period, all nearby devices would create a special 'contact event number' for sharing, which as time restricted and stored on the local device accordingly.⁸⁵

Therefore, in summary, all of these applications were designated to help prevent the pandemic from spreading and collect certain socio-demographic data, such as user gender and age⁸⁶, and some of them also gathered geolocation data from users' devices.⁸⁷ Accordingly, as seen, there were many countries across the World, which relied on contact tracing applications to fight the pandemic, and each of the contact tracing applications had its own characteristics. As said, in order to analyse the privacy aspects of the European approach, it is significant to understand the implementations performed across the globe as well. That being said, we would like to reiterate that this research will merely investigate the data protection matters resulting from the use of European contact tracing applications. Thus, in the following sections, we will have a scrutiny at the general data processing aspects of the European contact tracing applications and related regulations deployed within the EEA and in Spain particularly.

⁸⁴ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.* p.4,

⁸⁵ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.* p.4,

⁸⁶ See BBVA, (2020) How do Covid-19 tracing apps work and what kind of data do they use, available at: <https://www.bbva.com/en/how-do-covid-19-tracing-apps-work-and-what-kind-of-data-do-they-use/> (accessed on 15 August 2022).

⁸⁷ Oliver, Nuria; Lepri, Bruno; Sterly, Harald; Lambiotte, Renaud; Deletaille, Sébastien; De Nadai, Marco; Letouzé, Emmanuel et al. (2020). "Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle", *Science advances*, vol. 6, n.23, eabc0764, pp.1-6, p.4.

2. Location or proximity contact tracing

One of the most debated aspects of contact tracing applications were scattered around use of location and proximity method for the tracking activities. In more detail, while pursuing these objectives, the majority of contact tracing applications functioned primarily through either Bluetooth signals or geo-location software, enabling device-to-device tracking to identify individuals who came into contact with someone diagnosed with the Covid. Consequently, the handling of location data raised significant data privacy implications for both those managing and those subject to the data. As the natural outcome of such divergence in the processing methods, we can categorize these applications into two distinct groups as location-based contact tracing and GPS based contact tracing applications, whose details are outlined below



- Location-based contact tracing: Mobile devices possess the ability to determine their own location using built-in functionalities.⁸⁸ To provide better services, contact tracing applications have to carry out on

⁸⁸ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) "Contact tracing: An overview of technologies and cyber risks", *arXiv preprint arXiv:2007.02806*, pp.1-26, p.7.

consistent and seamless basis both indoors and outdoors.⁸⁹ Among these capabilities smartphones leverage their on-device capabilities, notably GPS, for precise location identification, functioning optimally outdoors with an accuracy of approximately two meters, albeit with limited efficacy indoors.⁹⁰ For indoors where most encounters happen, device-side cell tower multilaterate and crowd-sourced Wi-Fi localization (+/-10m) can be used. However, detecting GPS signals with high spatial accuracy indoors is difficult, resulting in the app being unreliable precisely in scenarios where virus transmission is most likely.⁹¹

- Proximity-based contact tracing: While Location-based contact tracing necessitates precise geographical positioning, yet technologies like Bluetooth and Wi-Fi enable the estimation of relative smartphone proximity by emitting a short-range signal that nearby devices can detect and register, with Bluetooth reaching up to 50 meters outdoors and 25 meters indoors.⁹² In other words, it is a method of determining the distance (proximity) to other devices using Bluetooth Low Energy (BLE).⁹³ This method simply serves as a benchmark selection criterion due to its typically higher accuracy compared to GPS based alternatives. Among its advantages are the ability to identify close contacts with a slightly lower false positive rate than GPS, its minimal

⁸⁹Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2021) "Effectiveness modelling of digital contact-tracing solutions...", *op.cit.*, p.856.

⁹⁰ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) " Contact Tracing...", *op. cit.*, p.6.

⁹¹ European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic", VIGIE 2021-0649 Framework Contract SMART 2019/0024, Lot 2, p.41.

⁹² Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) " Contact Tracing...", *op. cit.*, p.6.

⁹³ European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.41.

power consumption, and its higher adoption rate.⁹⁴ The reason being is it is challenging to measure GPS signals with high spatial resolution indoors, causing the app to be ineffective precisely in scenarios where virus transmission is most probable.⁹⁵ For privacy-preserving goals in mind, whose nuances will be later detailed in this thesis, the widely accepted approach at the outset was that, these applications ought to compute the relative, rather than the absolute location of users.⁹⁶ Correspondingly, proximity based mechanism was preferred by most of the European countries and those who chose a decentralized approach employed the DP-3T framework, and subsequently adopted the Exposure Notification API developed by Google and Apple, in accordance with information outlined by the European Commission.⁹⁷

Interestingly, both methods rely on the same process of exchanging anonymized key codes to locate close contacts.⁹⁸ Nonetheless, it is noteworthy that while some devices employed both options, which is not common in the EEA though, the majority relied on either Bluetooth or GPS based tracking. As such, the main focus of the processing choice of research will be scattered around Bluetooth and GPS based technologies.

Alternatively, as another method of tracing, we would like to introduce geofencing, which is a tracing technology that implements through surrounding a particular geographical zone with a virtual fence from the centre

⁹⁴ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) " Contact Tracing...", *op. cit.*, p.6.

⁹⁵ European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.41.

⁹⁶ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) " Contact Tracing...", *op. cit.*, p.6.

⁹⁷ Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020 Available at: https://health.ec.europa.eu/system/files/2020-07/mobileapps_202006progressreport_en_0.pdf (accessed on 23 June 2024) p.7.

⁹⁸ Hsu, Jeremy (2020) "The Dilemma of contact-tracing apps: Can this crucial technology be both effective and private?", *IEEE Spectrum*, vol. 57, no. 10, pp 56-59, p.59.

of its location points by setting a latitude, longitude, and radius.⁹⁹ This technology supplies device detection once passing the limits of the surrounded geographical zone, that could help to trigger the device's information and could warn its user once passing virtual fence of the so-called area.¹⁰⁰ Suitably, geofencing can be implemented in three different methodology, namely, GPS, Wi-Fi, and Bluetooth, each with its own methods and systems. Additionally, geo-fencing is executed on mobile devices.¹⁰¹ This method includes the continuous positioning of the mobile device as well as the continuous matching of the mobile's position with a set of geofences.¹⁰² As the real life use thereof, more assertive measures have been devised to geofence individuals in quarantine, utilizing dedicated smartphone applications or simpler methods like phone calls or text messages that reveal the user's geolocation.¹⁰³ However, it was not preferred by the most of the contact tracing applications.

Also, within the similar vein of alternative solutions, base station options could also be utilized, which is being implemented via telecommunication operators supplying anonymous cell phone base station data to the government, which is fundamentally used to estimate and monitor the overall trend epidemic.¹⁰⁴ The data is depending on the location of the base station could relatively

⁹⁹ Min-Allah, Nasro; Alahmed, Bashayer Abdullah; Albreek, Elaf Mohammed; Alghamdi, Lina Shabab; Alawad, Doaa Abdullah; Alharbi, Abeer Salem; Al-Akkas, Noor; Musleh, Dhiaa and Alrashed, Saleh (2021) "A survey of COVID-19 contact-tracing apps". *Comput Biol Med.*, vol.137, 104787, pp.1-11, p.8.

¹⁰⁰ *Ibid.*, p.8.

¹⁰¹ Rahate, Sachin W., and Shaikh, M. Zafar (2016) "Geo-fencing infrastructure: Location based service", *International Research Journal of Engineering and Technology*, vol. 3, no. 11, pp. 1095-1098, p.1095.

¹⁰² *Ibid.*

¹⁰³ Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital contact tracing applications and techniques: A review post initial deployments", *Transportation Engineering*, vol.5, 100072, pp.1-9, p.4.

¹⁰⁴ Ocheja, Patrick; Cao, Yang; Ding, Shiyao and Yoshikawa, Masatoshi.(2020) "Quantifying the Privacy-Utility Trade-offs in COVID-19 Contact Tracing Apps", arXiv preprint arXiv:2012.13061, pp.1-14, p.2.

thoroughly determine the mobility of users, yet as the accuracy insufficient, it could only be utilized to assist to judge close contacts.¹⁰⁵ Likewise, Wi-Fi fingerprinting is another comparable method that uses the received signal intensity from each Wi-Fi network to produce a "fingerprint" of each location,¹⁰⁶ which were not preferred by the EEA countries either.

Hence, as seen, there were various types of contact-tracing frameworks developed, adhering to regional compatibility, acceptability, privacy, and security laws.¹⁰⁷ Most of these solutions rely on sensors to either identify the user's close contacts to monitor the spread of the epidemic or track the users' locations, thereby tracking solutions.¹⁰⁸ As such, these applications require different permissions or sensory input to either flag or alert users about imminent virus transmission threats.¹⁰⁹ However, as reiterated earlier that the most used methodology by contact tracing applications were GPS and Bluetooth based tracking technologies, therefore, our discussions on the privacy intrusiveness of the methods will focus on these two major solutions.

Correspondingly, on the back of the brief introduction of fundamental technologies enabling digital contact tracing, we are of view that it is significant to highlight based on EU Commission data, controllers' privacy policies and other data protection related documentation that none of the EEA countries opted for GPS tracking, other than the Norwegian application. To provide a brief background on Norwegian application, which will be further referenced in Chapter 3, 4 and 5, where necessary, there were concerns about data protection aspects of processing raised by the Norwegian Data Protection Agency that led to the application's discontinuation in June 2020. The reason

¹⁰⁵ Ocheja, Patrick; Cao, Yang; Ding, Shiyao and Yoshikawa, Masatoshi (2020) "Quantifying the Privacy..." , *op. cit.*, p.2.

¹⁰⁶ *Ibid.*

¹⁰⁷ Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital contact tracing applications and techniques..." , *op.cit.*, p.4.

¹⁰⁸ *Ibid.*

¹⁰⁹ *Ibid.*

being is probably the similar to others utilizing the same approach, as these systems employed GPS to collect position information, uploaded it to a central database, and follow users' movements in real-time.¹¹⁰ That being said, right after its discontinuation, Norway introduced another application, i.e., Smittestopp v2, reliant on the GAEN API, which used a decentralised model different than the previous version.¹¹¹

However, regarding the rest of the applications, as mentioned, none of them opted for GPS tracking. For example, the controller of the Dutch¹¹² application used the rolling proximity indicators were transmitted and received via Bluetooth Low Energy ("BLE") and were thus used in combination with the signal strengths of both transmission and reception to determine the distance between users, and the duration of the Bluetooth contact. Within the similar vein, the data controller of the German application used a similar approach¹¹³, considering that as soon as data subjects allowed their smart mobile phones' COVID-19 exposure notification system, their smartphone transmitted this exposure data via Bluetooth, which other smartphones in their surrounding could record.

Likewise, the controller of the Irish¹¹⁴ application relied on Google-Apple exposure notification (GAEN) enabled users' phone to generate and share random IDs. These random IDs are shared when data subjects are in contact with other app users, and all the other applications, i.e., Stopp Corona App in

¹¹⁰ Hoeksma, Jon (2020) "Norway forced to backtrack on mass surveillance track and trace app." Digital Health , available at: <https://www.digitalhealth.net/2020/06/norway-track-and-trace-app/> (accessed on 15 June 2024).

¹¹¹ European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.41.

¹¹² Corona Melder, Privacy Policy <https://coronamelder.nl/en/privacy> (accessed on 3 September 2022) Section 4.

¹¹³ Corona Warn Privacy Notice exposure data section Corona Warn, Privacy <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).

¹¹⁴ Corona Alert, Privacy Statement, Section 3, para 1, <https://coronalert.be/en/privacy-statement/> (accessed on 15 August 2022).

Austria, StopCovid in France, and similar ProteGo applications in Poland were all based on the Bluetooth technology known as a sort of ‘digital handshake’.¹¹⁵

As such, to summarize, details on the architecture of the applications tracking via different channels are an integral part of the contact tracing application that needs to be analysed carefully from a data protection perspective. Accordingly, although the eHealth Network¹¹⁶ advised the use of Bluetooth-based location anonymously, and the EDPB recommended that the priority should be processing without collecting localization data via Bluetooth¹¹⁷, in which we will have a deep-dive into through Chapter 3, 4 and 5 to critically analyse both approaches from a regulatory perspective, in order to discover the most optimal solution under regulatory landscape, subsequent to this high level introduction. Also, the risk associated with location data will be scrutinized in Chapter 2 to have more clarity on details of inherent risks posed thereby.

3. Architecture of the Applications

In addition to tracing methodology discussions, architectural choice of data controllers, i.e., processing activities with centralized, decentralized or hybrid protocols do have several implications for data controllers, processors and data subjects from the data protection perspective. In the EDPB guideline, the distinction between the decentralized and centralized protocols was set out pertaining to data processing activities of contact tracing applications.¹¹⁸

¹¹⁵ StopCovid-ProteGo Documents, Privacy Policy <https://www.gov.pl/web/protegosafe/dokumenty> (accessed on 23 June 2024).

¹¹⁶ eHealth Network (2020) Mobile applications to support contact tracing in the EU’s fight against COVID-19 Common EU Toolbox for Member States https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf (accessed on 23 June 2024).

¹¹⁷ For further information see EDPB (2020) Guidelines 04/2020, *op.cit.* p.15.

¹¹⁸ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

Therefore, to analyse the data protection aspects thereof, it is, first, required to understand the logic of decentralized and centralized processing.

Accordingly, to simply indicate the fundamental distinction between the centralized and decentralized architecture, one can think that in the centralized system, public institutions gather data on a single server, where data matching takes place.¹¹⁹ On the other hand, decentralized systems, when user apps are in close vicinity, get proximity IDs from the server (in certain situations, users may produce these identifiers locally), which they publish or exchange with other user applications. The unique codes generated by a contact event are stored on each person's device in the decentralized approach instead of being sent to a centralized server.¹²⁰ While the centralized approach has this constant assumption that individual user data, which could be leaked through the application is the most notable risk, the decentralized approach deems the compromising of all the user data in one location as the largest risk,¹²¹ whose further details will be catered in the next chapter.

Fundamentally, as per the opinion of many scholars, centralized and decentralized approaches do possess quite alike implementations, apart from the server in the decentralized approach that knows the temporary IDs of infected users, rather than the temporary IDs which an infected user has contacted with.¹²² Any digital contact tracking system's central server may have access to the user's personal or personally identifiable information i.e. phone number, postal code, etc. Thus, there is a significant risk of losing

¹¹⁹ Kaya, Emre Kursat (2020) "Safety and Privacy in the Time of COVID-19: Contact Tracing Applications." Centre For Economics and Foreign Policy Studies, Cyber Governance and Digital Democracy 2020/05/EN, pp.1-11, p.3.

¹²⁰ Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital contact tracing applications and techniques..." , *op.cit.*, p.4.

¹²¹ Duke TechPolicy Sanford Article (2021) "Comparing centralized and decentralized contact-tracing approaches" available at: <https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/> (accessed on 17 March 2024).

¹²² *Ibid.*

users' control on data protection in case these datasets are not saved in an encrypted format,¹²³ whose details will be also elaborated in Chapter 2. Consequently, pseudonymous identities were used in digital contact tracing systems and protocols described. These identifiers may be of types, one related completely with an example of user, app proper from the registration phase and another that is produced for the purpose of sharing vicinity identities between two adjacent user applications/devices.¹²⁴

To provide further information on the merits of centralized system, the changes are in the location and timing of the checks for possible positive encounters. After receiving authorization from a health authority, an infected user's app uploads their received (and/or sent) identifiers to the server, and another user who wants to check their exposure status can either wait for a direct notification from the server (or a person in the case of a human-in-the-loop system like TraceTogether of Singapore detailed above), or request the server by passing their sent (and/or received) identifiers. As such, in comparison to the central servers of decentralized protocols, the central servers in a centralized system take on a more significant role. Accordingly, France¹²⁵, Hungary, and Norway¹²⁶ opted for the centralized option. Some of the European countries that opted for a centralized approach used the public protocol ROBERT or another specific protocol.¹²⁷ In summary, the ROBERT protocol employs a "centralized" method, wherein phones, whose owners are declared to be infected upload their lists of recent contacts to a central server

¹²³ Chakraborty, Pranab; Maitra, Subhamoy; Nandi, Mridul and Talnikar, Suprita (2020) "Contact Tracing in Post-Covid World: A Cryptologic Approach", Singapore: Springer, pp.1-134, p.31.

¹²⁴ *Ibid.*

¹²⁵ Tous Anti-Covid Privacy, Legal Basis and Regulatory Nature of the Processing Section, <https://bonjour.tousanticovid.gouv.fr/privacy-en.html> (accessed on 22 March 2024).

¹²⁶ Smittestopp (Norway) Privacy Policy, available at <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy> (accessed on 11 August 2023).

¹²⁷ Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020 available at: https://health.ec.europa.eu/system/files/2020-07/mobileapps_202006progressreport_en_0.pdf (accessed on 23 June 2024), p.7.

so that those phones can be notified.¹²⁸ For example, unique numerical identifiers can be randomly generated instead of using conventional means of identifying phones or their owners, and they may be changed at regular intervals.

Nonetheless, there are other different types of centralized protocols such as ROBUST and privacy-preserving proximity tracing protocols jointly developed by the researchers at Fraunhofer in Germany and INRIA in France. It fundamentally has the same principle as the Bluetrace protocol, which is a protocol that logs Bluetooth encounters between participating devices to enable contact tracing while protecting users' personal data and privacy.¹²⁹ Once two participating devices meet, they exchange messages with temporary, non-personally identifiable identifiers.¹³⁰ The main difference lies in the idea that the data stored on the ROBERT server are anonymous identifiers called Ephemeral IDs. The notification step often requires the user to check her used EphID to see if they have been exposed to an infected person. Or as another alternative for another centralized solution, we can also call out PEPP-PT, which was based on using a system architecture that does not require the collection of location data.¹³¹ Rather, the backend carry out the proximity tracing process once a diagnosed user uploads their list of observations for the contagious period and the backend retrieves the long-term pseudo-identifiers of users at risk from the reported and initiates a

¹²⁸ Europe Technology Policy Committee Statement On Essential Principles And Practices For Covid-19 Contact Tracing Applications available at: <https://www.acm.org/binaries/content/assets/public-policy/europe-tpc-contact-tracing-statement.pdf> , p.1.

¹²⁹ Bay, Jason; Kek, Joel; Tan, Alvin; Hau, Chai Sheng; Yongquan, Lai; Tan, Janice and Anh Quy, Tang (2020). "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders." *Government Technology Agency-Singapore, Tech. Rep, Vol. 18, no. 1, pp.1-9, p.1.*

¹³⁰ *Ibid.*

¹³¹ Vaudenay, Serge (2020) "Analysis of DP-3T between scylla and charybdis." Cryptology ePrint Archive, Paper 2020/399, <https://ia.cr/2020/399>, pp.1-12, p.1.

process to notify them if their exposure level is sufficiently high.¹³² Therefore, as seen, there is no one-for-all centralized data processing method for contact tracing applications.

On the other hand, the decentralized system, and Bluetooth is one of the major technologies used in digital contact tracing activities.¹³³ In particular, as per the European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP))¹³⁴, decentralized databases are required for the data controllers. Similarly, the EU Commission seemed to be more supportive of the decentralised solution at the first glance, which it says is more suitable with data minimisation principle,¹³⁵ whose details will be analysed during the next chapter. Accordingly, based on the EU Commission data, it is possible to state that approximately ninety percent of EEA/EU member countries use the decentralized system.¹³⁶

As for the main features of this system, any server engaged in the contact tracking system is only allowed to collect the contact information or pseudonymous identifiers of users that have been determined as infected because of a valid evaluation by health officials and the user's voluntary action.¹³⁷ Alternatively, the server keeps a list of pseudonymous identifiers or

¹³² Troncoso, Carmela ; Payer, Mathias; Hubaux, Jean-Pierre ; Salathé, Marcel; Larus, James R. ; Lueks, Wouter ; Stadler, Tanja et al. (2020) "Decentralized Privacy-Preserving Proximity Tracing" (2020) "Decentralized Privacy-Preserving Proximity Tracing", IEEE Data Engineering Bulletin , vol.43, n.2, pp. 36-66, p.62.

¹³³ Scrivano, Noemi; Gulino, Rosario Alfio and Giansanti, Daniele (2022) "Digital Contact Tracing and COVID-19..", *op.cit.*, p.2.

¹³⁴ European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html, (accessed on 23 June 2024), para. 52.

¹³⁵ Policy Department for Economic, Scientific and Quality of Life..., *op.cit.*, p.4.

¹³⁶ See European Commission, Mobile Contact Tracing Apps in the EU https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en, (accessed on 23 June 2024).

¹³⁷ EDPB (2020) Guidelines 04/20, *op.cit.*, p.8.

contact histories of affected users only long enough to inform potentially infected individuals of their exposure, without attempting to identify them.¹³⁸ Accordingly, this approach has been favoured by some scholars, as the matching process occurs on users' smartphones instead of a central server, ensuring greater anonymity¹³⁹, as they believe that centralized model gives health authorities more oversight and information regarding disease spread and social connections between virus-exposed individuals.¹⁴⁰ That being said, it is important to note that in terms of privacy, as per the EDPB, both the centralized and decentralized methods have the capacity to comply with personal data protection regulations, although the decentralized approach often offers a higher level of adherence and respect for data protection measures.¹⁴¹ Therefore, we are of view that it is not possible to conclude this discussion with generic ideas without further deep dive into the data protection principles of the GDPR. Accordingly, as said, we will analyse and address these details in Chapter 3 and 4 by elaborating the nuances of processing activities with different architecture choices.

Furthermore, pertaining to the components of the decentralized approach, the employed protocols were DP3T, GAEN, TCN, Whisper Tracing, and PACT (East cost) and PACT (West cost).¹⁴² These protocols were used by most of the European apps, such as Germany, Italy, Belgium, Estonia and many others.¹⁴³ These protocols and decentralized architectures are designed to

¹³⁸ EDPB (2020) Guidelines 04/20, *op.cit.*, p.8.

¹³⁹ BBC Website, Technology <https://www.bbc.com/news/technology-53485569> (accessed on 11 August 2022).

¹⁴⁰ Hernández-Orallo, Enrique; Cano, Juan Carlos; Calafate, Carlos T. and Manzoni, Pietro (2020) "Evaluating the effectiveness of COVID-19 Bluetooth-Based smartphone contact tracing applications", *Applied Sciences*, vol.10, no. 20, 7113, p.5.

¹⁴¹ Hernández-Orallo, Enrique; Cano, Juan Carlos; Calafate, Carlos T. and Manzoni, Pietro (2020) "Evaluating the effectiveness of COVID-19..." *op. cit.* p.5.

¹⁴² Jiang, Ting, Yang Zhang, Minhao Zhang, Ting Yu, Yizheng Chen, Chenhao Lu, Ji Zhang, Zhao Li, Jun Gao, and Shuigeng Zhou (2022) "A survey on contact tracing: the latest advancements and challenges", *ACM Transactions on Spatial Algorithms and Systems (TSAS)* vol. 8, no. 2 , p.1-35, p. 11.

¹⁴³ Veale, Michael (2020) "Sovereignty, Privacy, and Contact Tracing Protocols", Meatspace Press, pp.35-39. p.37.

address cyber security issues in wireless technology.¹⁴⁴ In more detail, some user privacy techniques contain a physical layer that conceals certain measurements of users, enhanced security keys that establish temporary identifications, and differential privacy which brings the noise to the adjusted structures of data,¹⁴⁵ which many scholars find positive at the first glance, in relation to the breaches concerning the fundamental privacy rights of whole European Union citizens stipulated under the article 8 of the Charter of Fundamental Rights¹⁴⁶.

Another component of the decentralized versus centralized processing discussion is the fate of the data processed and its retention. For instance, the Pan-European Privacy-Preserving protocol (PEPPPT) is a centralized solution, which utilizes the proximity tracing concept among phones of users of applications by measuring BLE radio signals to assist in the limitation of contagious viruses' expansion.¹⁴⁷ In line with the logic, the devices store only each other's anonymous identifiers.¹⁴⁸ Correspondingly, the advocates of decentralized systems support the idea that the data in the centralized system increases the power of governments to monitor citizens¹⁴⁹, as briefly touched above and will be further detailed in Chapter 2. Having said that, the reason why we wanted to remind this statement is that some decentralized systems

¹⁴⁴ Jahmunah, Vinesh; Sudarshan, Vidya K.; Oh, Shu Lih; Gururajan, Raj; Gururajan, Rashmi; Zhou, Xujuan; Tao, Xiaohui et al. (2021) "Future IoT tools for COVID-19 contact tracing and prediction: a review of the state-of-the-science", *International journal of imaging systems and technology*, vol. 31, no. 2, pp. 455-471, p.465.

¹⁴⁵ *Ibid.*

¹⁴⁶ Article 8 of the Charter of Fundamental Rights: protection of personal data.

¹⁴⁷ Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2020) "Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control", 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 229-235, p. 233.

¹⁴⁸ *Ibid.*

¹⁴⁹ See Duke TechPolicy Sanford Article (2021) "Comparing centralized and decentralized contact-tracing approaches" available at: <https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/> (accessed on 17 January 2023).

might be centralized in nature depending on the underlying algorithm and how users are admitted.¹⁵⁰ Ultimately, the server is unable to notify those who contacted infected individuals and must trust phones instead.¹⁵¹ Thus, as a response to that, the privacy-preserving decentralized protocol, i.e., DP-3T, has been developed by several European academic institutions, in conjunction with the Swiss Federal Institutes of Technology (ETH Zurich and the EPFL of Lausanne),¹⁵² which was preferred by many controllers due to its efficiency and Bluetooth based approach. However, as seen, there are plenty of different methods of operationalizing these techniques, both for centralized and decentralized, depending on the region and country, each of which generates different data protection considerations. For example, the Slovenian application mentioned the fact that the application is reliant on randomly generated keys by means of the Bluetooth Low Energy technology received by other smartphones in the surrounding, thereby relying on the decentralized version as well.¹⁵³ Or differently, the German application indicated the exposure notifications transmitted exposure data by the Bluetooth technology with the other mobile phones in the surrounding, which is also reliant to decentralized approach with different Bluetooth protocol.¹⁵⁴ Having said that Czech application sets forth the following in their privacy policy regarding the Bluetooth technology and certain concerns around their methodology, “the eRouška application is designed in such a manner that it

¹⁵⁰ Ocheja, Patrick; Cao, Yang; Ding, Shiyao and Yoshikawa, Masatoshi (2020) “Quantifying the Privacy...”, *op. cit.*, p.4.

¹⁵¹ See Duke TechPolicy Sanford Article (2021) “Comparing centralized and decentralized contact-tracing approaches” available at: <https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/> (accessed on 17 March 2024).

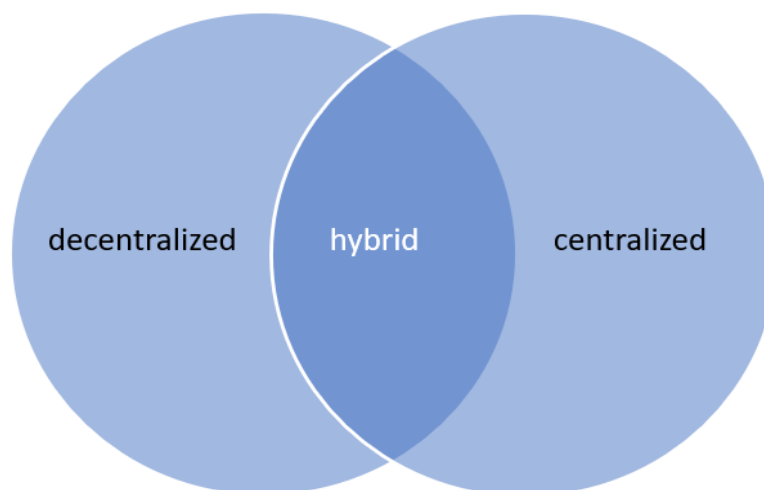
¹⁵² Blasimme, Alessandro; Ferretti, Agata and Vayena, Effe (2021) "Digital contact tracing against COVID-19 in Europe: current features and ongoing developments" *Frontiers in Digital Health*, vol. 3, no.61, pp.1-10, p.2.

¹⁵³ OstaniZdrav Privacy Notice Section 7-b, para 4, available at: <https://www.gov.si/assets/vlada/Koronavirus-zbirno-infografike-vlada/APP-OstaniZdrav/Privacy-notice.pdf> (accessed on 23 June 2024).

¹⁵⁴ Corona Warn, Privacy <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).

completely minimizes the set of data processed and the risk of their abuse.... Nevertheless, the use of Bluetooth technology (which is, however, necessary for the functioning of the Application) entails certain risks and related conditions of operation, which are described below".¹⁵⁵ Therefore, as seen, although majority of the European applications opted for decentralized versions, there are also other nuances that needs to be carefully analysed.

However, it is important to highlight that in addition to centralized versus decentralized discussions, between the two approaches, there are several possible middle-ground, i.e. hybrid approaches that intend to achieve a balance among public health utility, technological feasibility, and user data protection.¹⁵⁶



This middle ground divides into two rough categories: centralized storage of de-identified data and decentralized storage of personally identifying data.¹⁵⁷ The most prevalent middle-ground approach in the United States context involves the storage and collection of personal data, including identifying info

¹⁵⁵ eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application <https://erouska.cz/en/podminky-pouzivani#osobni> (accessed on 23 June 2024), section "risks linked to application's use"

¹⁵⁶ Kahn, Jeffrey P. "Digital contact tracing for pandemic response....", *op...cit.* p. 38.

¹⁵⁷ *Ibid*,p.38.

and location data, on the mobile phone of users.¹⁵⁸ This decentralized but personally identifiable data can then be voluntarily shared with public health officials if the user tests positive for COVID.¹⁵⁹ Also, there are certain limitations faced by both options, which become centralized by nature. As seen, it is another reason why hybrid approaches inevitably appeared in the first place, yet we must state that this was not preferred by many countries, other than France and Norway.

Moreover, given the closeness of both approach, it is plausible to state that the main common concerns of centralized and decentralized systems relate to security and data protection concerns, technical limitations, and potential abuse of third party companies¹⁶⁰ as detailed in Chapter 2. Nonetheless, regarding its implementation, for instance, as for decentralized system, the initial implementation of the BLE function on Apple showed that mobile phones typically do not permit centralized applications operating in the background to access and upload the complete history of all detected contacts.¹⁶¹ The COVID-19 app would need to be running in the foreground on unlocked mobile devices under the pre-13.5 version of Apple's operating system, or using the BLE mode would need to be avoided, both of which would have a negative impact on battery life. In centralised decision-making models, risk analysis is performed at the server end.¹⁶² Due to these technical restrictions, a number of nations and centralised protocol bodies (PEPPPT) shifted to a decentralized strategy after a while. In similar vein, the UK government also declared that it is leaving a centralized NHS contact tracing application for England and changing it to a decentralized version, based on

¹⁵⁸ Kahn, Jeffrey P. "*Digital contact tracing for pandemic response....*", *op...cit.*, p.38-39.

¹⁵⁹ *Ibid.* p. 39.

¹⁶⁰ European Parliament Briefing ITRE in Focus, National COVID-19 contact tracing apps available at [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI\(2020\)652711_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf) (accessed on 23 June 2024), p.2.

¹⁶¹ European Parliament Briefing ITRE in Focus, National COVID-19 contact tracing apps, p.2.

¹⁶² Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2021) "Effectiveness modelling of digital contact-tracing solutions...", *op.cit.*, p.853.

the Apple Google toolkit, due to challenges in solving technical problems by themselves.¹⁶³

Hence, in short, considering the aforementioned introductions and details on the architecture of the applications, the data processing methodologies, and the related opinions of the EU institutions as well as the scholars in the field, it is visible that both approaches have certain privacy implications under the GDPR, ePrivacy Directive and the other relevant privacy guidance for the contact tracing activities. Thus, an in-depth analyse regarding the fulfilment of the European privacy standards will be performed in Chapter 3, 4 and 5 on this matter to deliver clear outcomes and recommendations. Also, the risk associated with the architecture of the applications will be scrutinized in Chapter 2.

4. Pseudonymization and Anonymization

Pseudonymization and anonymization practices of data controllers, among other crucial points, are of massive significance to protect personal data of users, as part of the European data protection approach. To be more specific, article 6.4 of the GDPR lists five elements that can be taken into account in this assessment¹⁶⁴ (the list is not exhaustive though); and the existence of safeguards such as pseudonymisation is listed as one of them.¹⁶⁵ To this end, alongside with the EDPB guideline and the European Commission recommendations, the World Health Organization published an advisory

¹⁶³ White, Lucie, and van Basshuysen, Philippe (2021) "Privacy versus public health? A reassessment of centralised and decentralised digital contact tracing", *Science and Engineering Ethics*, vol. 27, no. 2, pp. 23-26, <https://doi.org/10.1007/s11948-021-00301-0>, p.23.

¹⁶⁴ For the full article see Article 6.4 of the GDPR. more specifically, article 6.4.e of the GDPR sets out the following: "the existence of appropriate safeguards, which may include encryption or pseudonymization".

¹⁶⁵ Kamocki, Paweł, and Siegert, Ingo (2022) "Pseudonymisation of speech data as an alternative approach to GDPR compliance", *Proceedings of the LREC 2022 Joint Workshop on Legal and Ethical Issues in Human Language Technologies and Multilingual De-Identification of Sensitive Language Resources (LEGAL-MDLR 2022)*. Marseille, 20 June 2022, pp. 17-21. European Language Resources Association (ELRA), p.18.

guide regarding contact tracing applications,¹⁶⁶ which also covers crucial matters such as the effectiveness of contact tracing applications and the environmental factors that will affect the efficiency of contact tracing applications were discussed. Accordingly, the WHO set forth several measures to be considered among other security of the processing¹⁶⁷ the necessity for pseudonymization and anonymization requirements are deemed important tools to confront this necessity,¹⁶⁸ whereas at the same time the Article 29 Working Party examined a variety of data anonymization techniques and made it clear what precautions data processors and controllers must take.¹⁶⁹ all of which will be scrutinized across Chapter 3 and 4.

However, in line with the introductory nature of this Chapter, we would like to call out the fundamental aspects and features of pseudonymization and anonymization approaches are taken by the controllers. To indicate the fundamental rationale behind the pseudonymization and anonymization techniques in different processing structures of the applications, for example, with a decentralized system, registration is typically not deemed necessary, as, the apps' anonymized proximity data collection would continue to reside on users' mobile devices.¹⁷⁰ Suitably, to alert anyone who may have been infected with the virus, only the pseudonym IDs of the affected users assigned by the software could be posted to central servers.¹⁷¹ On the other hand, for

¹⁶⁶ For the full article, see World Health Organization, (2020) “Ethical consideration to guide the use of digital proximity tracing technologies for COVID-19 contact tracing interim guidance 28 May 2020” available at: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 (accessed on 23 June 2024).

¹⁶⁷ World Health Organization, (2020) “Ethical consideration to guide the use of digital proximity” op.cit., p.3.

¹⁶⁸ Recital 28 of the GDPR, Introduction of Pseudonymisation.

¹⁶⁹ Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymization Techniques. Adopted on 10 April 2014 (wp216).

¹⁷⁰ See Office of Privacy Commissioner for Personal Data, Hong Kong (PCPD), Data privacy issues relating to COVID-19 contact tracing apps https://www.pcpd.org.hk/english/news_events/newspaper/newspaper_20210329.html (accessed on 23 June 2024).

¹⁷¹ *Ibid.*

PEPP-PT centralized protocol, once the app is installed on a mobile device, it may start generating and transmitting a time-specific pseudo-random temporary ID.¹⁷² This temporary ID also includes the encrypted persistent pseudonym, which can only be decrypted by the server.¹⁷³ While running in the background, this app captures the signals of other BLE devices that have the app installed and exchanges temporary IDs with each other. Each app in a mobile device then continues to keep a list of their temporary IDs, each representing a contact. For each contact, the system determines the duration and the distance between the devices based on the signal output power sent by the transmitting device. Accordingly, as for the practice of application data controllers, most of the tracing applications employ pseudonymous identifiers for proximity contacts and change them periodically, for example, every 30 minutes or so.¹⁷⁴ For example, the Norwegian application was reliant on Temporary Exposure Keys, which are subject to change every twenty-four hours and these keys are used to create new one-way keys called Rotating Proximity Identifiers every ten to twenty minutes.¹⁷⁵ Similarly as mentioned above, Irish or German applications, and many other counterparts using temporary exposure keys were also reliant on this pseudonymized approach. Likewise, the Dutch app mentioned their implementation of pseudonymization by stating that¹⁷⁶ all identification keys were pseudonymized. In more detail, in order to minimize the risk of identifying a user, when exchanging the RPI, the smartphone's MAC address was converted to a pseudo-MAC address, a randomly generated code that changes every 10-20 minutes, just like the RPI,

¹⁷² Chowdhury, Mohammad Javed Morshed; Ferdous, Md Sadek; Biswas, Kamanashis; Chowdhury, Niaz and Muthukkumarasamy, Vallipuram (2020). "COVID-19 contact tracing: challenges and future directions", *IEEE Access*, vol. 8 , pp 225703-225729, p.225710.

¹⁷³ *Ibid.*

¹⁷⁴ EDPS (2020), TechDispatch #1/2020: Contact Tracing with Mobile Applications https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en, (accessed on 23 June 2024) .

¹⁷⁵ Smittestopp Privacy Policy, available at <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy> (accessed on 11 August 2023)

¹⁷⁶ Corona Melder, Privacy Policy, op.cit., Section 4.

be replaced.¹⁷⁷ Similarly, the Slovenian contact tracing application used of daily keys and transmit codes by transmit codes and randomly assigned daily keys.¹⁷⁸ Within the same remit, the Lithuanian application provided two important explanations about the use of pseudonymised data processed by the app.¹⁷⁹ Among other specifications in short, the controller stated that the national contact tracing and warning applications interface and receives pseudonymised personal data of infected person (the infected person's keys, the country of origin of the keys, the related parties of the keys, and the information on confirmation of infection).¹⁸⁰ and 'Requests of the App user to correct, delete, restrict management of personal data in the App, objections to the management of the App data and to transferability of the data could not be carried out because there is no way to identify the user by pseudonymous personal data used in the app. For this reason, the application user cannot require withdrawing their consent to manage their pseudonymous personal data in the application, as there is no way to identify that user.

However, we would like to highlight that not all data controllers utilized pseudonymous data for the tracing activities. For instance, Croatian application did not rely on pseudonymized data, but rather it relied on communication with encrypted and secure channels, and the storage of personal data in a database as a separate logical unit with enforced security policies of the highest standards.¹⁸⁰ Likewise, Slovakian application did not employ pseudonymization for the processing activities, but rather implemented anonymous network that can identify which devices have encountered each other to connect devices that come within close proximity.¹⁸¹

¹⁷⁷ Corona Melder, Privacy Policy, op.cit., Section 4.

¹⁷⁸ OstaniZdrav, Privacy Policy, op.cit., Section 7-b, para 4.

¹⁷⁹ Korona Stop Application Privacy Policy <https://koronastop.lrv.lt/uploads/documents/files/corona-stop-app/Privatumo-politika-korona-stop-en.pdf> (accessed on 23 June 2024), section 12.

¹⁸⁰ Stop Covid Privacy Notice *op. cit.* Section 7.

¹⁸¹ Zostaň Zdravý ,General Information Document, Mobilná aplikácia Covid19 Zostaň Zdravý - Koronavírus A Slovensko (Gov.Sk), Section "Aplikácia ako pomoc pre udržanie situácie" <https://korona.gov.sk/mobilna-aplikacia-covid19-zostan-zdravy/> (accessed on 2 June 2024).

Therefore, as seen, there were various approaches for pseudonymization of personal data as well. In summary, the reason we wanted to introduce different practices is to show that controllers in the EEA have varied approaches for both pseudonymization, and these matters will be addressed and clarified further in the following chapters, as called out earlier.

With regards to the anonymization portion of the discussions, having a look at the applications' controllers, it is plausible to state that a few of the applications also relied on this method, rather than deletion. They, for sure, used this technique as part of the different processing phases of personal data, but essentially, most of them implementing anonymization has different approaches. For instance, the Austrian data controller indicated that they intended to delete or anonymize your personal information once it is no longer necessary for the purposes of contact tracing.¹⁸² Nevertheless, some of the data controllers also relied on this method for statistical purposes. Particularly, the German application was reliant on the anonymization method for using the processed data for statistical purposes, as indicated in their privacy policy.¹⁸³ Similarly, the Czech application relied on anonymization for the purpose of collecting aggregated statistical information about the effectiveness of digital contact tracing activities,¹⁸⁴ and Danish public health authorities can assess the impact of the application by observing, in a summarized and anonymous manner, the number of individuals who have downloaded the app and opted to disclose a positive test result to their close contacts within the app.¹⁸⁵ Differently, as another usage of anonymization techniques, the Belgium, Cyprus, Estonia, Finland, France and many other applications were reliant on anonymised interactions across the phones used

¹⁸² Stopp Corona Application, Section 6. <https://www.austria.info/en/service-and-facts/coronavirus-information> (accessed on 10 February 2021).

¹⁸³ Corona Warn, Privacy Notice, op.cit., Section I.

¹⁸⁴ eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, Ordinary Operation of eRouška Application <https://erouska.cz/en/podminky-pouzivani#osobni> (accessed on 10 October 2022).

¹⁸⁵ Denmark Smittestop Privacy Policy, For what purposes can my data be used? <https://smittestop.dk/databeskyttelse> , (accessed on 11 August 2022).

by data subjects to send out relevant warnings to the users on the Bluetooth technology, as detailed in their privacy policies of each, and report of the EU Commission.¹⁸⁶

Hence, to summarize the above, on the back of the aforementioned introductions and details on the pseudonymization and anonymization of the controllers, and introductory information on the existence of different practices, we will provide tailor-made recommendations for their efficient use, and deliver an in-depth analyses regarding the fulfilment of the European data protection standards in Chapter 3 and 4. Also, the risk linked to these features, alongside with the others detailed so far, will be scrutinized in Chapter 2.

5. Data Storage and Management

Within the similar context of the aspects introduced above, data storage and management, among others, are also significant parts of the compliance activities with the GDPR requirements set out under the principles relating to process of personal data.¹⁸⁷ Accordingly, it has implications on the data privacy aspects of the applications. In more detail, as elaborated in the following sections that contact tracing applications are obliged to adhere to key rules and principles of the EU law such as the GDPR and the e-Privacy Directive that cover the proportionality of the measure in terms of duration and scope, limited data retention, data minimization, data deletion, purpose limitation, genuine anonymization of data, and app use is voluntary and based on people opting in,¹⁸⁸ in addition to what EDPB and EU Commission guidance set out for these matters, which creates a two-fold approach for data

¹⁸⁶ For the full information on these anonymization usage, see European Commission Digital Contact Tracing Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic VIGIE 2021-0649 Framework Contract SMART 2019/0024, Lot 2 available at: <https://commission.europa.eu/system/files/2023-02/DigitalContactTracingStudy.pdf> (accessed on 28 April 2024), and privacy policies of referred applications, i.e., Corona Alert, CovTracer-EN, HOIA, Koronavilkku, TousAntiCovid respectively.

¹⁸⁷ Article 5-1-e, storage limitation.

¹⁸⁸ Ponce, Aida (2020) "COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim", *ETUI Research Paper-Policy Brief*, vol. 5, p.3.

controllers in general, as the importance of keeping data accurate is also set out under the GDPR¹⁸⁹, as for data management aspects thereof.

As briefly introduced above, in practice of contact tracing apps, as a general background, the structure that contact tracing applications are subject to is more complex because these applications are followed by both health institutions and various government institutions. Correspondingly, third-party service providers that develop the application also play various technical roles as an intermediary during the implementation of the application may be exposed to the personal data collected by the application, as elaborated in Chapter 2. For instance, some governments across the World such as Australia applied for the aid of Microsoft and Amazon for storage issues,¹⁹⁰ or as described above, in line with our research jurisdiction, many European countries utilized Google-Apple infrastructure. To be more specific, for example, the Estonian¹⁹¹ and Irish applications¹⁹² thoroughly indicated the details of third-party companies involved in the process as part of their storage and architecture providers, which was one of the most heated debates as detailed in the following chapters. Accordingly, as part of these third-party involvements, Apple and Google announced in early April 2020 that they were also working on contact tracing technology.¹⁹³ Moreover, to provide further detail on this third-party supported implementation, as discussed by Leith and Farrell, Google's Firebase which was used to supply application configuration settings, and Google's SafetyNet service was used to assess handset integrity

¹⁸⁹ Article 5-1-d of the GDPR, accuracy.

¹⁹⁰ See ABC website, Amazon to Provide Cloud Services For Coronavirus Tracing App <https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682> (accessed on 12 June 2024).

¹⁹¹ HOIA Phone Application Privacy Policy *op. cit.* Section 2.

¹⁹² Health Service Executive Application Privacy <https://www2.hse.ie/services/covid-tracker-app/data-protection-information-notice.html> (accessed on 23 June 2024) Section 9.1.

¹⁹³ Sharon, Tamar (2021) "Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers." *Ethics and Information Technology* 23, no. Suppl 1, pp. 45-57. p.48.

in the ProteGO Safe (Poland) app.¹⁹⁴ This means that data is handled by at least two parties: Google (who runs the Firebase and SafetyNet technology) and the health authority, which operated the client app.¹⁹⁵ Similarly, Firebase Analytics was used by the Apturi Covid application of Latvia to track user interactions with the client app.¹⁹⁶ Likewise, the information sent to backend servers by contact tracing apps was in use in Denmark, Germany, Spain, Austria, Poland, Latvia, Italy, and Ireland to assess user privacy.¹⁹⁷ As a high level background, these applications were consisting of two separate parts, namely a “client” application implemented by the national public health authority and the GAEN service, which was run by Google and is part of Google Play Services for Android devices.¹⁹⁸ Accordingly, as part of the GAEN system, the system performs these functions without retaining the precise locations of these interactions to protect user privacy.¹⁹⁹ Moreover, it restricts the reported exposure duration for each encounter to intervals of five minutes, with a maximum cumulative total of thirty minutes.²⁰⁰ Accordingly, Germany, Italy, and Switzerland also deployed exposure-notification apps based on GAEN.²⁰¹ On the other hand, Norway, France, and Hungary did not utilize GAEN architecture, as per the EU Data.²⁰² Thus, as seen, there were different approaches for third party provided infrastructures across the

¹⁹⁴ Leith, Douglas J., and Farrell, Stephen (2021) "Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps", *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, IEE, pp. 1-10, p.2.

¹⁹⁵ *Ibid.*

¹⁹⁶ Leith, Douglas J., and Farrell, Stephen (2020) "Contact Tracing App Privacy...", *op. cit.*, p.2.

¹⁹⁷ Leith, Douglas J., and Farrell, Stephen (2020) "Contact Tracing App Privacy...", *op. cit.*, p.2.

¹⁹⁸ *Ibid.*

¹⁹⁹ Hsu, Jeremy (2020). "The Dilemma of contact-tracing apps: Can this crucial technology be both effective and private?" *IEEE Spectrum*, vol. 57, no. 10, pp. 56-59, p.58.

²⁰⁰ *Ibid.*

²⁰¹ Leith, Douglas J., and Farrell, Stephen (2020) "Contact Tracing App Privacy...", *op. cit.*, p.2.

²⁰² For the full details on architectures used by the applications see European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, Annex II, Country Research, p.120-p.190.

controllers of the applications, whose details will be analysed in the following chapters.

As another introductory information on different aspect of the data storage and management matters, the Commission called out the importance of the technical and organizational safeguards, namely the proximity data must be exclusively generated and stored in encrypted and pseudonymized formats on the individual's terminal device in addition to state of art cryptographic techniques.²⁰³ Correspondingly, as introduced above, the Czech application utilized pseudonymized keys in a manner that access to pseudonymized infected person keys sent by the eRouška server was limited to the EU, the Ministry, and users.²⁰⁴ Similarly, the Croatian app employed random keys that only left the user's device with verified infection and user approval, ensuring no link to the user's identity,²⁰⁵ whose details were kept remaining in the user device accordingly. Likewise, Italian controller indicated that the data stored on the device are encrypted,²⁰⁶ or Belgium controller stated that the IP addresses of users who downloaded or uploaded keys are deliberately excluded from all logs and storage systems.²⁰⁷ Therefore, as seen, it is highly possible to vary these samples with the other applications, but in line of the purpose this chapter, we are only intending to call out the most remarkable ones based on their data management nuances.

To this end, we believe that it is crucial to introduce two-fold approach of the controllers regarding data storage and management issues, which will be evaluated in Chapter 3 and 4 in detail. In more detail, as the first approach,

²⁰³ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).

²⁰⁴ eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, *op.cit.*, Ordinary Operation of eRouška Application Section, Section 'Who Has Access Your Data'.

²⁰⁵ Stop Covid Privacy Notice *op. cit.* Section 7.

²⁰⁶ Immuni's High-Level Description, Privacy, p.10.

²⁰⁷ Corona Alert, Privacy Statement, Section 4, IP Address, <https://coronalert.be/en/privacy-statement/> (accessed on 23 January 2024).

some of the controllers implemented the data-first approach, which generally involves assigning a stable identifier to each individual (or smartphone device) and transmitting some or all details of their movements and contact interactions to a central server, where they can be accessed and analysed.²⁰⁸ On the other hand, as the other prevalent alternative, namely the privacy-first approach, in contrast, uses dynamic identifiers for individuals which are changed regularly, and stores their contact interactions in a cryptographically secure manner on their local device, keeping little or no data in a centralized server.²⁰⁹ To be more specific, in their data-focused approach, some contact tracing applications even aimed to have an access the photos on the phone of people.²¹⁰ Generally speaking, applications requesting such accesses are applications that authenticate through uploaded documents. To indicate the reflection of these approaches on the privacy policy of the applications on a high level, for example, the Slovenian application ²¹¹ listed several permissions related to android mobile phones, iPhone mobile phones and all the other phones, and the Lithuanian application²¹² follows the same logic to display the details of permissions and features the application required. Similarly, the French application mentioned that although authorization might be required for using QR codes of the application, there is not any personal data (photo or video belonging to the user) is stored or transmitted by the app, only the content of the QR Code is used as part of the application.²¹³

Lastly, as another introductory part, with regards to the data storage and retention periods of the applications, based on their privacy policies, many data controllers implemented data retention periods limited with fourteen days. As also presented by the table in the research of Blasimme, Ferretti and

²⁰⁸ Fahey, Robert A., and Hino, Airo (2020) "COVID-19, digital privacy, and the social limits on data-focused public health responses." *International Journal of Information Management*, vol. 55, p.102181.

²⁰⁹ Fahey, Robert A., and Hino, Airo (2020) "COVID-19, digital privacy...", *op.cit.*, p.102181.

²¹⁰ Fahey, Robert A., and Hino, Airo (2020) "COVID-19, digital privacy...", *op.cit.*, p.102181.

²¹¹ OstaniZdrav Privacy Notice *op. cit.* Section 9.

²¹² Korona Stop Application, *op. cit.* section 7.

²¹³ Tous Anti-Covid Privacy, *op.cit.*, Legal Basis and Regulatory Nature of the Processing Section,

Vayena that Switzerland, Italy, Germany, Ireland, the Netherlands, Scotland, England, Wales and France opted for fourteen days of the retention period.²¹⁴ Similarly, the Austrian application mentioned that data on the end device were to be deleted after fourteen days. Once a sick note has been submitted, data subjects' data would be retained for thirty days after the submission of that report.²¹⁵ Likewise, Denmark²¹⁶, Latvia²¹⁷ as well as Finland²¹⁸ applications ensured data erasure within fourteen days. Similarly, Spanish App Covid Radar indicated that temporary public keys and temporary Bluetooth identifiers are stored on the device for fourteen days and then deleted, and temporary public keys submitted to our servers by users with a positive COVID-19 diagnosis would also be deleted from our servers after fourteen days.²¹⁹ Accordingly, it is plausible to highlight that there are multiple varying aspects of data storage and management matters across the European application, due to many factors. Thus, as a result of the aforementioned introductions and details on the data storage and management of the applications, an in-depth analyse regarding the fulfilment of the EU privacy standards will be performed in Chapters 3,4 and 5 to provide certain recommendations from a regulatory compliance perspective. Also, the risk associated with data management and storage practices within the scope of digital contact tracing activities will be scrutinized in Chapter 2.

²¹⁴ Blasimme, Alessandro; Ferretti, Agata and Vayena, Effy (2021) "Digital contact tracing against COVID-19 in Europe: current features and ongoing developments" *Frontiers in Digital Health*, vol. 3, no. 61, pp. 1-10, p.3.

²¹⁵ Stopp Corona Application <https://www.austria.info/en/service-and-facts/coronavirus-information> (accessed on 10 February 2021).

²¹⁶ See Smittestopp Processing of Personal Data available at: <https://smittestop.dk/en/data-protection/> (accessed on 11 January 2024).

²¹⁷ Apturi Covid Privacy Policy <https://apturicovid.lv/privatuma-politika/#en> section 7 (accessed on 23 June 2024).

²¹⁸ See Koronavilkku Privacy <https://koronavilkku.fi/en/privacy/> (accessed on 22 January 2023).

²¹⁹ See Radar Covid, Privacy Policy, section 7 <https://radarcovid.gob.es/en/privacy-policy> (accessed on 23 June 2024)

6. Obligation to Use Contact Tracing Applications

One of the most heated debates surrounding contact tracing applications centred on whether their use should be mandatory or voluntary basis. More specifically, within the context of obligation to use contact tracing applications, even though, downloading contact tracing applications to mobile phones was obliged for their citizens by many countries in the World, the EDPB²²⁰ and the EU Commission²²¹ were proponents of the idea that the downloading of these applications to phones should be based on volunteerism, as further elaborated in Chapter 5. In this context, both EPDB and Council of Europe has also set forth in the guide that the use of contact tracing applications by EU citizens should only be possible on a voluntary basis,²²² whose details will be addressed in the following chapters.

That being said, in the existing literature, for some scholars who are proponents of the public health, using these apps on mandatory seems more beneficial for all citizens to download the contact tracing applications. Their reasoning could probably be found in the sense that leveraging technologies pertaining to contact tracing activities might alter the course of the COVID-19 pandemic.²²³ In other words, from a public health perspective, technological evolution must not be prevented, and both public health and ethical ground encourage changes targeting enhancing the efficiency of contact tracing applications against the spread of the virus.²²⁴ On the other hand, from a data

²²⁰ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.4.

²²¹ See eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf (accessed on 23 June 2024).

²²² Alessandra Pierucci, Jean-Philippe Walter (2020) "Joint Statement on Digital Contact Tracing...", *op.cit.* p.4.

²²³ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy with public digital contact tracing during the COVID-19 pandemic" *Lancet Digit Health*, vol. 2, n.7, doi: 10.1016/S2589-7500(20)30133-3, pp 342-344, p. 343.

²²⁴ Blasimme, Alessandro; Ferretti, Agata and Vayena, Effy (2021) "Digital Contact Tracing...", *op.cit.* p.2.

protection risk perspective, as reiterated by the Commission and the EDPB, the choice should be voluntary-based only, as detailed in Chapter 4. Therefore, in summary, mandatory use, among other things, often viewed by many as conflicting with European legal regulations and ethical principles that prioritize the significance of individual privacy.²²⁵ Accordingly, many of the EEA countries did not oblige their citizens to download contact tracing applications on a mandatory basis. While some of the controllers demonstrated such voluntariness in their privacy policies and terms of use documents, other remained silent but determined not to oblige the individuals to use the applications. To name a few of the countries indicating voluntary behaviour in their policies as well, for instance, Croatia's²²⁶, Germany's²²⁷, Spain's²²⁸ and Belgium's²²⁹ applications indicated that the use of these applications was based on voluntariness. Or similarly, the Norwegian application Smittestopp called out that the use of Smittestopp is completely voluntary, and one can forfeit using Smittestopp at any time and stop receiving notifications of infection from others.²³⁰ Likewise, the Slovenian²³¹ or Lithuanian²³² applications showed its stance on voluntariness by setting out that the use of the is on voluntary basis. As said, the rest of the EEA countries, other than a very few early samples, i.e. Portugal, which will be indicated in this section, left the decision of downloading these applications to their citizens, thereby applied the voluntary approach as well.

²²⁵ Blasimme, Alessandro; Ferretti, Agata and Vayena, Effy (2021) "Digital contact tracing against COVID-19 in Europe: current features..." op.cit., p.2.

²²⁶ Stop Covid Privacy Notice, op.cit., section 6.

²²⁷ Corona Warn, Privacy Notice, op.cit., section 2.

²²⁸ See Radar Covid, Terms of Use, Section 2 <https://radarcovid.gob.es/en/privacy-policy> (accessed on 23 June 2024)

²²⁹ Corona Alert, Privacy Statement, op.cit., Section 3, para 1.

²³⁰ Smittestopp Privacy Policy, op.cit., section 1.

²³¹ OstaniZdrav, privacy policy, op.cit., section "Functioning of the Application", para 1.

²³² Korona Stop Application, Privacy Policy, op.cit., section 2.

Having said that, there were different approaches on the issue of voluntary use of applications across the World. For example, China and South Korea, opted for mandatory approach, as these countries considered it necessary for their citizens to download these applications to their mobile phones to tackle the pandemic.²³³ Similarly, in Thailand, as briefly introduced above, the AOT Airport application was mandatory for individuals travelling from or returning from contagious areas outside Thailand; they must download it before passing through the immigration checkpoint.²³⁴

Moreover, as additional piece of background information, in line with such variety in the controllers' implementation across different jurisdictions, we would also like to highlight the divergence of the individuals' approaches on the mandatory use of this applications. More specifically, existing contact tracing applications classify three groups of individuals with various inclinations for acceptance, namely critics, undecided, and advocates.²³⁵ They argue that precisely targeting different groups is impractical because only one set of tracking app specifications needs to be developed for all citizens.²³⁶ As such, we believe that some countries seemed to oblige individuals to use this applications to prevent such divergences in the implementation of contact tracing applications, whereas the others, i.e. the EEA/EU countries seemed to be impacted by critics of the applications.

As such, returning to our research jurisdiction, we would like to be more specific with the real-life example of voluntariness in the EEA. To this end, we

²³³ Kim, Youngrim; Chen, Yuchen and Liang, Fan (2021) "Engineering care in pandemic technogovernance: The politics of care in China and South Korea's COVID-19 tracking apps", *New media & society*, vol. 25, n.6, pp. 1432-1450, p.1433.

²³⁴ Norton Rose Fulbright, (2021) Contact Tracing Apps: new world for Privacy, Thailand section.

²³⁵ Kouliaridis, Vasileios; Kambourakis, Georgios; Chatzoglou, Efstratios; Geneiatakis, Dimitrios and Wang, Hua (2021) "Dissecting contact tracing apps in the Android platform", *Plos one*, vol.16, no. 5, pp.1-28, p.2.

²³⁶ *Ibid.*

believe Portugal's case²³⁷ was one of the most important samples of indicating the volunteer-based approach to contact tracing applications, as briefly touched above. To provide a brief background on this, in Portugal, the government tabled bill 62/XIV before the national parliament.²³⁸ This bill would make it mandatory for people with compatible devices to use the app Stayaway Covid in professional and educational settings and put various police authorities in charge of enforcement. Subsequent to the submission of this bill, the Parliament accordingly asked the Commission the following questions:

- Does the Commission believe that making the installation of this type of app mandatory is in line with the GDPR Framework?
- Is imposing a fine of up to EUR 500 consistent with the principle of proportionality, one of the pillars of the rule of law?

As such, on the back of these questions directed to the Commission to gauge the potential feasibility of mandatory approach, it became evident that due to the significant intrusiveness and the associated challenges, including establishing suitable safeguards, meeting the criteria of necessity, appropriateness, and proportionality is difficult.²³⁹ Therefore, the Commission advised using voluntary applications. Therefore, Portugal, and all the other countries, in line with the direction of the European Commission²⁴⁰ and the

²³⁷ For the full discussions See Question for written answer E-005833/2020 to the Commission Rule 138 Lúcia Pereira (PPE), Paulo Rangel (PPE), José Manuel Fernandes (PPE), Álvaro Amaro (PPE), Maria da Graça Carvalho (PPE), Cláudia Monteiro de Aguiar (PPE) Subject: Mandatory installation of contact tracing apps and personal data protection during pandemic https://www.europarl.europa.eu/doceo/document/E-9-2020-005833_EN.html (accessed 11 November 2022).

²³⁸ *Ibid.*

²³⁹ Mandatory installation of contact tracing apps and personal data protection during pandemic <https://politique.pappers.fr/question/mandatory-installation-of-contact-tracing-apps-and-personal-data-protection-during-pandemic-QECR884915?q=> (accessed on 16 August 2022).

²⁴⁰ See eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf (accessed on 23 June 2024).

guideline published by the EDPB,²⁴¹ left the download of these applications based on volunteerism, and this is stated by many countries as mentioned above. Hence, the issue of whether the current practice within the EU is operated on a strictly voluntary basis, is of massive importance from the regulatory perspective, whose further implications will be analysed in Chapter 3,4 and 5. Also, the risk linked to obligation of use data will be scrutinized in Chapter 2.

7. Transparency and Accountability of the Contact Tracing Applications

In addition to the massive importance of accountability of data controllers and transparency of data processing activities within the scope of European approach²⁴², the significance of transparency requirement for the contact tracing activities within the EU was indicated by the joint statement of Chair of the Committee of Convention 108 and Data Protection Commissioner of the Council of Europe.²⁴³ They stated that given the invasive nature of digital contact tracing systems, it is strongly advised that full transparency be ensured through open-source development of the code, allowing interested parties to audit and potentially enhance it. Information communicated to individuals should be in clear, straightforward language. Consequently, as the key message, individuals retain the right to understand the rationale behind data processing, especially when it directly impacts them, as is the case with digital contact tracing.²⁴⁴

Hence, considering the above statement of the Committee of Convention 108 and Data Protection Commissioner of the Council of Europe, it is plausible to state that data protection statements of contact tracing applications are

²⁴¹ See EDPB (2020) Guidelines 04/2020, *op.cit.* p.7.

²⁴² For the further details of these principles, see respectively Article 5-1-a and 5-2 of the GDPR, lawfulness, fairness and transparency and principle of accountability.

²⁴³ For the full statement see Pierucci, Alessandra, Jean-Philippe Walter, and Data Protection Commissioner (2020) "Joint statement on digital contact tracing." *Council of Europe*. https://epic.org/wp-content/uploads/privacy/covid/Covid19_joint_statement.pdf (accessed on 26 May 2024).

²⁴⁴ Alessandra Pierucci, Jean-Philippe Walter (2020) "Joint Statement on Digital Contact Tracing...", *op.cit.* p.7.

playing a significant role in the privacy of the users, and as such, they are consisting of the ground rules for data processing activities taking place within the scope of use of contact tracing applications, whose legal implications and analysis will be addressed in Chapter 3. Data protection statements drafted and published by any data controller, including data controllers of contact tracing applications, indicate the lawful basis and purpose of processing alongside technical and organizational measures implemented, envisaged retain period of personal data collected and rights of data subjects considering that establishing user trust is pivotal for achieving widespread adoption of a contact tracing app, as it is this collective adoption that ultimately determines the app's effectiveness.²⁴⁵ Therefore, governmental agencies and private entities offering contact tracing applications are obliged to ensure that individuals receive adequate notice of their data protection and data security practices, also for their accountability obligation under article 5, 12 and 13 of the GDPR.²⁴⁶

Correspondingly, there are various remarkable aspects of data privacy statements of contact tracing applications, as individuals would potentially scrutinize the privacy statements of the contact tracing applications they use, to understand what kind of data is subject to share and in which ways their personal data is being protected.²⁴⁷ To this end, a short summary of some of these remarkable characteristics of the European contact tracing applications is provided herein to build the base of the further in-depth transparency and accountability analysis to be delivered in Chapter 3.

First of all, each of the contact tracing applications employed within the EEA seem to opt for a separated privacy statement regarding legal aspects of the

²⁴⁵ See Nat Law Review, Privacy Considerations Covid 19 Digital Contact Tracing <https://www.natlawreview.com/article/privacy-considerations-covid-19-digital-contact-tracing> (accessed on 10 August 2022).

²⁴⁶ Article 5, 12 and 13 of the GDPR respectively sets out the transparent information principle, information to be provided where personal data collected from data subjects or from another source

²⁴⁷ Zhang, Melvyn; Chow, Aloysius and Smith, Helen (2020) "COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies", *Journal of medical Internet research*, vol.22, n.12,e21572, pp.1-6, p.2.

processing activities, in addition to their terms of use and other technical specifications provided on their websites. To be more indicative, for example, Austria's Stop Corona App²⁴⁸, Czechia's eRouska²⁴⁹, the Danish Smittestop²⁵⁰, the Lithuania's Stop Korona²⁵¹, the Netherlands Corona Melder²⁵² Croatia's Stop Covid-19 app²⁵³ and many others are indicated the type of data processed, purpose of processing activities, data subject rights as well as potential legal explanations on the processing activities and other various details. Likewise, even some of the data controllers also provided a "third party components" data protection impact assessments in different tabs of their websites within scope of their transparent approaches. For instance, Norwegian²⁵⁴, Croatian²⁵⁵, Poland²⁵⁶ and German²⁵⁷ contact tracing applications were some prominent samples of this application, which surely targeted to support accountability of data controllers against data subjects and regulators.

²⁴⁸ See Stopp Corona Application, op.cit., section 2, 4 and 7.

²⁴⁹ eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, op.cit., section "Application's Purpose", "Your Rights", and "What Data Do We Work With And What Do We Do With Them".

²⁵⁰ Smittestopp Processing of Personal Data, op.cit., section 1, 5 and 8.

²⁵¹ Korona Stop Application Privacy Policy, op.cit., section 4, 5 and 12.

²⁵² Corona Melder, Privacy Policy, op.cit., Section 2.

²⁵³ Stop Covid Privacy Notice <https://stopcovid19.zdravlje.hr/html/privacy-policy.html> (last accessed on 10 August 2022).

²⁵⁴ Smittestopp Privacy Policy, Section 5. Disclosure of personal data to others.

²⁵⁵ For the full information see Stop Covid-19 app, third party components document <https://github.com/Stop-COVID-19-Croatia/stopcovid19-docs> (accessed on 23 June 2024).

²⁵⁶ ProtegoSafe- StopCovid, Privacy Policy, op.cit., "Most important information regarding your privacy" Section.

²⁵⁷ Corona Warn, Privacy Notice, op.cit., Section 9.

Similarly, considering the incentive of the EDPB related to considering data protection matters in the designing process from the beginning²⁵⁸, Belgium²⁵⁹, Germany²⁶⁰, Netherlands²⁶¹ applications indicated their selection of 'privacy-by-design' as the chosen method of design considerations. However, there seem not to be many members state data controllers of contact tracing applications clearly display their choice of privacy by design method, whose intricacies will be analysed in detail in Chapter 4.

In addition, as for the indication of accountability and the identity of the controllers, details of the controller as well as the assignment of a data protection officer was displayed under the privacy statement of some data controllers.²⁶² For instance, the Austrian contact tracing application did not appoint a data protection officer, just like the approach implemented by the Covid Radar, whose ambiguity in the role of data controllers and processors and lack of DPO will be reviewed under the AEPD decisions in Chapter 7, and many other European applications. As such, the Austrian application has chosen this path of not disclosing DPO details, but rather indicated that there is a designated role for data protection officer.²⁶³ On the contrary, some of the data controllers indicated this on their websites. With regards to the role of consent mechanism for processing activities, some countries, such as

²⁵⁸ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.11.

²⁵⁹ Coronaalert Privacy Policy, *op.cit.*, Section 4, and Section 9.

²⁶⁰ Corona Warn, Overview Security, Secure development <https://github.com/corona-warn-app/cwa-documentation/blob/main/overview-security.md> (accessed on 23 June 2024).

²⁶¹ Corona Melder, Privacy Policy, *op.cit.*, Section 2.

²⁶² Article 6 of the GDPR, lawfulness of processing.

²⁶³ See Stopp Corona Application, *op.cit.*, data protection officer

France,²⁶⁴ Germany,²⁶⁵ Austria²⁶⁶, and Belgium²⁶⁷, stated that the details of transactions based on the collected consents.

Differently, in another remit, each of the privacy statement documents of the EU countries provided specific references to the GDPR, in particular regarding the protection of data subject rights ensured by this Europe-wide legislation.²⁶⁸ For instance, the Irish application privacy policy declared that the application operates on a voluntary basis, and its data processing is founded on consent, specifically Article 6(1)(a) of the GDPR for personal data processing and Article 9(2)(a) of the GDPR for the processing of special categories of personal data, particularly health-related information.²⁶⁹ Likewise, the privacy notice of the Italian application Immuni declared compliance with Articles 13-14 of the GDPR and respect for the principles of privacy, i.e., purpose limitation, and data minimization.²⁷⁰ Similarly, the Latvian application indicated that the application shall not receive or process the location data. To register a contact, the minimum information related to the Bluetooth technology is processed.²⁷¹ Likewise, the Lithuanian application aimed adherence to the principle of data minimization, emphasizing that the app was created to process minimal data.²⁷² Furthermore, the Slovenian application OstaniZdrav

²⁶⁴ Tous Anti-Covid Privacy, Legal Basis and Regulatory Nature of the Processing Section, <https://bonjour.tousanticovid.gouv.fr/privacy-en.html> (accessed on 22 March 2024).

²⁶⁵ Corona Warn, Privacy <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).

²⁶⁶ Stopp Corona Application <https://www.austria.info/en/service-and-facts/coronavirus-information> (accessed on 10 February 2021).

²⁶⁷ See Corona Alert Privacy Policy <https://coronalert.be/en/#home-privacy> (accessed on 23 January 2024).

²⁶⁸ Blasimme Alessandro, Ferretti Agata and Vayena Effy (2021) "Digital Contact Tracing...", op. cit., p.6.

²⁶⁹ Blasimme Alessandro, Ferretti Agata and Vayena Effy (2021) "Digital Contact Tracing...", op. cit., p.6.

²⁷⁰ *Ibid.*, p.7.

²⁷¹ Korona Stop Application Privacy Policy, op.cit., section 5.

²⁷² Korona Stop Application Privacy Policy, op.cit., section 5.

stated that it solely processed contact data generated and stored by users' mobile phones when the application's exposure logging feature was enabled.²⁷³ Alternatively, the Norwegian contact tracing application²⁷⁴ indicated the measures taken on the data minimization matters by specifying the type of data collected.²⁷⁵ As per the statement, the data controller specified the information that is processed on the users' mobile phone and processed by the Norwegian Institute of Public Health. The controller mentioned, among other things, that the Norwegian Institute of Public Health would not store the information processed after the "session" has ended.

Furthermore, in relation to the purpose limitation principle, Poland²⁷⁶, French,²⁷⁷ Belgium²⁷⁸ and the Dutch²⁷⁹ data controllers were some of controllers that indicated the purpose of processing their privacy notices elaborately. For instance, while the Dutch data controller displayed that their application was developed as an addition to source and contact tracing activities, and the goal of the app was to rapidly and straightforwardly notify users with heightened risk of infection, whereas ensuring their privacy was highly protected. Differently, in the meantime, the French data controller showed this fact by enumerating the purposes of the processing, i.e., informing a person using the application who has been near at least one other user of the same application who has subsequently been diagnosed positive for the Covid-19 virus, raising an awareness among users of the application on the symptoms of this virus, guiding risky contacts with the correct course of actions, producing statistics in order to adapt the measures necessary to face the epidemic and to improve the performance of the application and the

²⁷³ OstaniZdrav Privacy Notice, op.cit., Section 7-b, para 4.

²⁷⁴ SmitteStop Privacy Policy, op.cit., section 2.3.

²⁷⁵ Smittestop Privacy Policy, op.cit. section 1.

²⁷⁶ StopCovid-ProteGo Documents, Privacy Policy, op.cit., Section 3, General Rules, Para 2.

²⁷⁷ Corona Warn, Privacy, op.cit., Section 6.

²⁷⁸ Corona Alert, Privacy Statement, *op. cit.* Section 3.

²⁷⁹ Corona Melder, Privacy Policy, op.cit., Section 2.

user experience; helping to generate supporting documents required by public authorities and keeping certificates of vaccination and negative / positive tests for Covid-19, recovery from Covid-19 and exemption to vaccination.²⁸⁰

Lastly, in relation to the indication of lawful basis by data controllers, which will be detailed in Chapter 3, most controllers articulated their choice of lawful basis of the processing activities. In more detail, for example, the data controller of the Spanish Radar Covid app outlined that the legal basis for data collection is tied to the strictly public health-related interests during a health emergency, with room for consent in certain areas. The collection aligns with essential interests for preserving people's lives, as specified in the privacy policy and in accordance with articles 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h), and 9.2.i).²⁸¹ Similarly for example, the data controller for the Belgian contact tracing applications cited the legal basis that the different processing activities of personal data within the notification process and the user registration for the contact tracing app are founded on grounds of public interest article 6.1 (e) of the GDPR and, specifically for health-related data, on grounds of public interest in the domain of public health (article 9.2 (i) of the GDPR).²⁸²

Likewise, data controller of the Finland contact tracing application did also state its legal basis of the processing by stipulating in their privacy statement that the processing of personal data is always based on valid legislation.²⁸³ Or differently, France's application similarly established the legal basis for processing under Article 6.1.e of the GDPR,²⁸⁴ and the Netherlands' ²⁸⁵ application displayed the basis of processing as a public duty, whereas many

²⁸⁰ Tous Anti-Covid Privacy, *op.cit.* Data Controller and Purpose Section.

²⁸¹ Radar Covid, Privacy Policy, Section 4, para 3.

²⁸² See Corona Alert, Privacy Statement, *op.cit.*, Section 3, para 1.

²⁸³ See Koronavilkku Privacy <https://koronavilkku.fi/en/privacy/> (accessed on 22 January 2023).

²⁸⁴ Tous Anti-Covid Privacy, *op.cit.*, section Legal Basis and Regulatory Nature of the Processing Section.

²⁸⁵ Corona Melder, Privacy Policy, *op.cit.* section 3.

EEA countries, especially Denmark²⁸⁶ and Estonia apps,²⁸⁷ demonstrated the nature of transactions conducted based on collected consents and assured the immediate possibility of revoking these consents upon request by the data subjects, all within the preview of the legal basis for processing. In summary, most of the EEA countries, such as Iceland²⁸⁸, Malta²⁸⁹, Portugal²⁹⁰, and many others, had either the regulation as a legal basis for the processing activities, or similarly opted for mixture of both regulation and consent, whereas also some controllers such as Cyprus²⁹¹, Ireland, Lithuania, Germany and Czechia opted mainly and predominantly for consent as a legal basis of processing activities.²⁹²

Therefore, in summary, as a result of the introduction and details on the transparency actions of the applications, which covers plenty of different aspects of their data protection compliance activities, the decision of whether or not there is still a margin for data controllers to enhance the level of details in the privacy policies of contact tracing applications employed within the EEA will be examined in Chapter 3 and 4. Also, the risk associated with the lack of transparency in the processing activities of contract tracing applications will be detailed in Chapter 2.

²⁸⁶ Smittestop (Denmark), Privacy Policy, op.cit., section 4.

²⁸⁷ HOIA Phone Application Privacy Policy, Section 7, para 1, and Section 13, para 1 <https://koodivaramu.eesti.ee/tehk/hoia/app-web/-/blob/master/content/privacy.en.md> (accessed on 23 June 2024).

²⁸⁸ Rakning Iceland Covid-19 Tracing App Privacy policy, section what is our legal basis of processing your personal data <https://island.is/en/o/directorate-of-health/app-privacy-policy> (accessed on 10 June 2024).

²⁸⁹ COVID Alert Malta, Privacy policy, para 3 <https://covidovidalert.gov.mt/privacy-policy/>. accessed on 19 April 2023).

²⁹⁰ Stayaway Covid, Privacy policy <https://stayawaycovidovid.pt/privacy-policy/> (accessed on 10 february 2022).

²⁹¹ CovTracer-EN, para 3 Privacy policy available at: https://covtracer.dmid.gov.cy/dmid/covtracer/covtracer.nsf/covtracer02_en/covtracer02_en?opendocument (accessed on 23 June 2024).

²⁹² Lintved, Mona Naomi (2021) "COVID-19 Tracing Apps as a Legal Problem: An Investigation of the Norwegian 'Smittestopp' App", Oslo Law Review, Vol 8. Issue 2, pp.69-87, p.81.

II.- DATA PROTECTION RISKS AND CONCERNS ABOUT CONTACT TRACING APPLICATIONS

1. General Digital Contact Tracing Risks

In Chapter 1, how the widespread use of the Internet technology, coupled with other rapid technological advancements, has significantly altered the methods of gathering, storing, and exchanging user information was introduced.²⁹³ In line with this change, difficulties for contact tracing now contain incomplete identification of contacts, complex data management requirements, and delays in steps from identification of contacts to the isolation of suspected cases among contacts²⁹⁴, from the operational considerations perspective. Nonetheless, in line with our research line, as briefly introduced in Chapter 1, there are considerable privacy issues associated with these applications, particularly improper use of location data may undermine public confidence in health authorities.²⁹⁵ Accordingly, it is evident that for these applications to be effective at mitigating the virus, there must be high uptake,²⁹⁶ and it is still not obvious how we might encourage people to utilize these applications,²⁹⁷ thereby mitigating the inherent risks and risk perceptions about the apps. Correspondingly, when intrusive aspects related to tracking and data storage are considered, it might be possible to reach to a suspicion that this would be

²⁹³ Paine, Carina; Reips, Ulf-Dietrich; Stieger, Stefan; Joinson, Adam and Buchanan, Tom (2007) "Internet users' perceptions of 'privacy concerns' and 'privacy actions'", *International Journal of Human-Computer Studies*, vol. 65, no.6, 526-536, p.526.

²⁹⁴ See Digital Tools for Covid-19 Contact Tracing, the WHO, p.1.

²⁹⁵ O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; Johnson, Kevin; Laffey, John; McNicholas, Bairbre; Nuseibeh, Bashar; O'Callaghan, Michael; O'Keeffe, Ian; Razzaq Aabdul; Rekanar, Kaavya; Richardson, Ita; Simpkin, Andrew; Storni, Cristiano; Tsvyatkova, Damyanka; Walsh, Jane; Welsh, Thomas and O'Keeffe, Derek (2021) "Best Practice Guidance for Digital Contact Tracing ..." *op.cit.*, p.8.

²⁹⁶ Walrave, Michel; Waeterloos, Cato and Ponnet, Koen (2020) "Adoption of a Contact Tracing App for Containing COVID-19", A Health Belief Model Approach. *JMIR Public Health Surveill.*, vol.6, n.3, e20572, doi: 10.2196/20572, pp.1-10, p.8.

²⁹⁷ Walrave, Michel; Waeterloos, Cato and Ponnet, Koen (2020) "Adoption of a Contact Tracing App....", *op.cit.*, p.8.

a clear violation of the GDPR requirements and, in any case, a serious threat that could hinder the adoption of the contact tracing application.²⁹⁸ Therefore in other words, tracking infected people and contact persons' activities could end up in breach of their right to privacy.²⁹⁹ Particularly, concerns about data security and confidentiality can escalate, particularly in a healthcare context.³⁰⁰ Hence, within the realm of this thesis, the forthcoming chapter will meticulously outline both the general and specific data protection risks entailed by the utilization of European contact tracing applications to indicate all potential risks associated therewith. By doing so, we aim to thoroughly examine existing risks, thereby facilitating the assessment of compliance activities undertaken by controllers through the following chapters.

The fundamental reason for such data protection risks and concerns could be found in the sense that compared to other sorts of demographic data, people are more sensitive to information about their own personal health.³⁰¹ Furthermore, people's data privacy worries regarding numerous health-related technology could worsen due to the potential misuse of their personal health information.³⁰² Therefore, it is of massive importance to identify the foreseeable harms and all possible efforts made to prevent these from arising over the course of the data cycle³⁰³, and consider the decisions concerning

²⁹⁸ Tedeschi, Pietro; Bakiras, Spiridon and Di Pietro, Roberto (2021) "IoTrace: a flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing", *IEEE Communications Magazine*, vol. 59, no. 6, pp. 82-88, p.82.

²⁹⁹ Mbunge, Elliot (2020) "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, n. 6, pp. 1631-1636, p.1635.

³⁰⁰ Walrave, Michel; Waeterloos, Cato and Ponnet, Koen (2020) "Adoption of a Contact Tracing App....", op.cit., p.7.

³⁰¹ Chopdar, Prasanta Kr (2022) "Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderator", *Health Policy Technol. Sep;11(3):100651.*,doi: 10.1016/j.hlpt.2022.100651. Epub 2022 Jul 15. PMID: 35855013; PMCID: PMC9283129, pp.1-13, p.4.

³⁰² Chopdar, Prasanta Kr (2022) "Adoption of Covid-19 contact tracing app...." op.cit., p.4.

³⁰³ Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing and surveillance during COVID-19." *General and child-specific ethical issues. UNICEF Office of Research*, pp. 1-26, p.22.

who is initially included in data processing as well as how data are managed and treated from the point of acquisition up to their final disposal,³⁰⁴ as detailed in the following Chapters of this thesis.

In more detail, regarding the general risks resulting from contact tracing applications, regardless of the technology being used for automating contact tracing, they all create the following potential risks at the outset, namely:

- Data protection/privacy risks, by disclosing the identities of users infected by COVID-19 and their whereabouts to revealing the real-world social network of an individual or part of the population.³⁰⁵
- Cybersecurity risks, through mostly abusing the system to target specific individuals or companies with false notifications leading to unnecessary quarantine.³⁰⁶

In addition to those main types, to be more specific with the data protection risk posed on individuals by the use of these applications, we are of view that what Legendre and colleagues provided is a clear delineation of the subset of data protection risk types on a high level, which can be categorized as follows:

- Health Status Privacy, in general, independent of the type of contact tracing system, the first risk is leaking the identities of users infected by Covid. This information is, by definition, highly sensitive and protected by medical secrecy. Therefore, ideally, it should remain accessible only to the infected users and the health authority. A related

³⁰⁴ Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing...." op.cit., p.22.

³⁰⁵ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) "Contact tracing.....", op.cit., p.7.

³⁰⁶ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) "Contact tracing.....", op.cit., p.7.

data protection risk is capturing the identities of users who have been in contact with an infected user, i.e., exposed users.³⁰⁷

- Location Privacy, as another data protection risk is learning a user's mobility traces. Locations visited by a user can reveal a lot of information about them, from their political and religious views to their social relationships. No system a priori need access to location data to perform contact tracing. Geolocation-based contact tracing systems do however require a location to infer proximity.³⁰⁸ As such, the apps with geolocation capabilities opens the door for this specific type of risks as well.
- Social Graph Privacy, learning a user's social graph represents the third main privacy concern. This can be learned either directly through proximity data between users (for Bluetooth-based systems) or by relying on location data (for location-based systems).³⁰⁹

However, from our perspective, in addition to the above-mentioned data protection risks, it is also significant to be aware of cyber risks, even if on a high level, considering that cybersecurity risks are closely related to the protection and security of personal data collected by data controllers, as detailed in the next sections of this chapter. Having said that, in line with the spirit of this research, while we are of the view that cybersecurity-related risks should be meticulously analyzed, as the interplay between data protection and cybersecurity is quite visible in many areas these days, in particular in the field of healthcare and data, our main focus will remain on the risks posed on personal data and privacy of individuals. Also, considering the above explanations on main risk headings resulted from contact tracing applications at the outset, we believe that there are also certain specific considerations that could scare data subject users about their data protection in general, as the use of contact tracing applications is novel. As such, to have more detailed

³⁰⁷ Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) "Contact tracing.....", op.cit., p.7.

³⁰⁸ *Ibid.*

³⁰⁹ *Ibid.*

insight regarding each type of concern associated with the use of the European contact tracing applications, in the following sections, each of these risks and concerns are elaborated. Correspondingly, through this Chapter nuances of risk framework regarding the apps will be illustrated to understand the underlying rationale of data protection risks resulted from the applications in line with the spirit of cutting-edge nature of contact tracing applications.

2. Location and Proximity Risks

As briefly introduced in Chapter 1, the utilization of location data somehow revolutionized the notion of contact tracing.³¹⁰ However, in doing so, for sure, it also brought new sort of risks that public health administrators as well as officials are still challenging with.³¹¹ Suitably, now, contact tracing apps collecting location data could reveal sensitive information such as home addresses, religious affiliations, political leanings, and other intimate details. As such, people have voiced concern about being stigmatized if personal details regarding a confirmed infection are disclosed to others.³¹² From our perspective, yet the risk-related processing of location data is not that straightforward. In other words, the main risk at stake is not entirely about the identification of whereabouts of users. The fundamental reason is that one of the concerns is the acquisition of location data has further ramifications, including the ability for organizations to track people's activities and draw conclusions about their routines and preferences.³¹³

³¹⁰ International Press Institute, Covid-19 contact tracing apps a threat to press freedom and journalists' privacy <https://ipi.media/guest-article-covid-19-contact-tracing-apps-a-threat-to-press-freedom-and-journalists-privacy/> (accessed on 23 January 2024).

³¹¹ *Ibid.*

³¹² Oyibo, Kiemute; Sahu, Kirti Sundar; Oetomo, Arlene and Morita, Plinio P. (2021) "Factors influencing the adoption of contact tracing applications: Protocol for a systematic review", *JMIR Research Protocols*, vol. 10, no. 6, e28961, pp.1-20, p.8.

³¹³ Kleinman, Robert A., and Merkel, Colin (2020) "Digital contact tracing for COVID-19." *Cmaj* 192, no. 24, pp. E653-E656, p.e654.

Accordingly, as per the classification of Raskar and colleagues, location privacy is described that the person would not want someone to be able to connect the different places they went in order to determine their location history without their agreement.³¹⁴ Although smartphone apps can conceal users' actual whereabouts and offer identity and location privacy by utilizing privacy-preserving mechanisms, still, for example, anonymization techniques eliminate identifiers from user requests, while obfuscation methods obscure or blur location information.³¹⁵ To be more accurate, indeed, location data can unveil a person's social connections and potentially deduce their activities at specific times, creating a fear that might discourage people from engaging in certain activities.³¹⁶ Thus, privacy concerns in this context involves considering both the infected individual and those at risk due to contact with them.³¹⁷ More specifically, location-aware services that are customized are the proliferation of GPS enabled phones, Wi-Fi location technology, and a rise in smartphone bandwidth have all sparked development. Therefore, as the sophistication of mobile devices grows, so is the ability of service providers to continuously track the location of their users, offering them services based on their exact physical location.³¹⁸

It is also stated by the European Commission that the existence of a Bluetooth based mechanism that processes data anonymously only on the machine owned by the person and destroys it after a certain period would be much more advantageous than a GPS system that processes location data, from

³¹⁴ Raskar, Ramesh; Dhillon, Ranu; Kapa, Suraj; Pahwa, Deepti; Falgas, Renaud; Sinha, Lagnojita; Prasad, Aarathi et al. (2020) "Comparing manual contact tracing and digital contact advice." *arXiv preprint arXiv:2008.07325*, pp.1-9, p.6.

³¹⁵ Freudiger, Julien; Shokri, Reza and Hubaux, Jean-Pierre (2011) "Evaluating the privacy risk of location-based services", *International conference on financial cryptography and data security*, Springer, Berlin, Heidelberg, pp. 31-46, p.32.

³¹⁶ Sharon, Tamar (2021) "Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers." *Ethics and Information Technology* 23, no. Suppl 1, pp. 45-57. p.46.

³¹⁷ *Ibid.* p.47

³¹⁸ Toch, Eran; Wang, Yang and Cranor, Lorrie Faith (2012) "Personalization and privacy..." *op. cit.*, p.209.

the location tracking related risks comparison.³¹⁹ To simplify their reasoning, from our perspective, in case the data processing activity was processed with an open and specific identification method, not anonymously, both parties could have information about each other's names and, therefore, their current health status through the aforementioned contact tracing applications while walking next to another person, as elaborated in the next chapter. This situation evidently leads to a serious source of concern for many people about the collection of their personal data in practice. Also, citizens are concerned about being tracked by data controllers that process this personal data processed via GPS. In concrete terms, there were initial concerns regarding the Government tracking people³²⁰. as detailed in Chapter 1, in Singapore and Australia, for example, QR codes were employed for contact tracing purposes, with residents using them to check in and check out of places they reach, containing shopping malls, restaurants, and their places of work.³²¹ It, as a result, raised the risk of providing data controllers with further capabilities of identifying people's exact whereabouts, and in conjunction with their identities.

Similarly, the Norwegian application³²² as the European counterpart of these applications in terms of the usage of GPS method, whose use exacerbated the location tracking concerns in the first place. We, accordingly, believe that such processing activities relying on GPS, or any sort of location related data are causing privacy intrusiveness for the users and concerns related to surveillance by governments and third-party organizations too. In other words, directly or indirectly, any hints related to the location of users that could be

³¹⁹ See Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (OJ L 114 14.04.2020, p.7).

³²⁰ Norton Rose Fulbright, (2020) Contact Tracing Applications in Australia, available at: <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/australia-contact-tracing.pdf?revision=9f35a88a-4124-4c48-b38f-68e86a187050> (accessed on 28 March 2023) p.1.

³²¹ BBC Website, Covid-19: China pushes for QR code based global travel system <https://www.bbc.com/news/business-55039662>,(accessed on 12 August 2022).

³²² The initial version of Smittestop application relied on GPS based processing activities, as mentioned in Chapter 1, sub-chapter 2.

associated with them could be massively hazardous in terms of respecting data protection. The reason is that enacting a public space mandate for digital contact tracing will raise concerns about the surveillance state, namely governments gathering increasingly sensitive data, in turn using those data to monitor residents and enforce the law.³²³ As such, these apps impinge on people's privacy as they collect, analyze, and have access to personal health data such as health behavior, status, traveling history, household coordinates positions, and location.³²⁴ From our perspective, the main cause of such risk is that such a general perception regarding the increased use of location data by advertisers or service providers augments the general understanding of such location-tracking risks. As a natural outcome of this situation, data subjects may feel less willing to download such applications. Although till our date, there has been no clear research merely dealing with this topic, we are still of view that people do not evaluate the detrimental privacy effects of contact tracing applications merely based on their experience with contact tracing activities. Instead, they mostly benefit from their prior experiences with different data collection activities to which they were subject within the scope of different types of services. The main reason of our claim is that as most individuals in society have never witnessed such pandemic scenarios, for those who witnessed, it was not really possible for them to associate their previous experience with the digitalization of contact tracing activities. Thus, it is understandable that users might even be biased regarding such data processing activities, which is a complement of the risk detailed in Transparency related risks. In this regard, to support our idea on the concerns of the users on location tracking with a concrete sample, the research of Simko and colleagues analyzed the COVID-19 contact tracing and privacy

³²³ Owen, Schaefer, G. and Ballantyne, Angela (2022) "Ethics of digital contact tracing wearables", *Journal of Medical Ethics*, vol.48, no. 9, pp. 611-615, p.614.

³²⁴ Mbunge, Elliot (2020) "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol.14, n. 6, pp. 1631-1636, p.1634.

concerns and preferences of participants,³²⁵ which indicated that many participants opted for proximity tracking due to security and data protection reasons.³²⁶ Therefore, as seen, location tracking seems to be an intimidation factor for the potential users due to privacy risks associated therewith, and clearly pronounced by individuals in society, even though through different channels.

Subsequently, in addition to the intrusiveness of tracking location information, there is also another risk related to the issue, namely the accuracy of the information provided by sources of location information related to mobile phones. To be more concrete, the location information of mobile phones includes different types with different characteristics: information with high coverage but low accuracy and information with high accuracy but limited availability.³²⁷ When calculating the possibility of contact using the location information, there is a possibility of false detection of a significant number of contacts if the location information with low accuracy is used.³²⁸ Additionally, a substantial amount of calculation time might be required to identify mobile phones that may have contact with mobile phones of infected persons, considering the considerable amount of location information for millions of devices that mobile phone carriers control.³²⁹ Particularly, to evaluate the possibility of contact with high accuracy, the computational cost is expected to increase in proportion to the length of time, temporal resolution, and

³²⁵ For the full details of the study see Simko, Lucy; Calo, Ryan; Roesner, Franziska and Kohno, Tadayoshi (2020) "COVID-19 contact tracing and privacy: studying opinion and preferences", *arXiv preprint arXiv:2005.06056*, pp.1-32.

³²⁶ *Ibid.*, p.18.

³²⁷ For further information see Ami, Junko, Ishii, Kunihiro; Sekimoto, Yoshihide; Masui, Hiroshi; Ohmukai, Ikki; Yamamoto, Yasunori and Okumura, Takashi (2021) "Computation of infection risk via confidential locational entries: A precedent approach for contact tracing with privacy protection." *IEEE Access* 9, pp.87420-87433, p. 87423.

³²⁸ Ami, Junko, Ishii, Kunihiro; Sekimoto, Yoshihide; Masui, Hiroshi; Ohmukai, Ikki; Yamamoto, Yasunori and Okumura, Takashi (2021) "Computation of Infection Risk...", *op.cit.*, p. 87423.

³²⁹ Ami, Junko, Ishii, Kunihiro; Sekimoto, Yoshihide; Masui, Hiroshi; Ohmukai, Ikki; Yamamoto, Yasunori and Okumura, Takashi (2021) "Computation of Infection Risk...", *op.cit.*, p. 87423..

geographic resolution used number of mobile phones and the number of infected patients for the assessment. As such, the use of these applications might result in sending misleading information to health authorities and health workers.³³⁰

Our initial view on this portion is that the accuracy of data related risk, at the first glance, is still less hazardous compared to the other types of risks such as location data-related risk or healthcare data-related risk. Nevertheless, it is an important type of risk to be considered, as per the GDPR definition,³³¹ as the principle of accuracy is also stipulated, and breaching this principle would constitute serious outcomes on the rights and freedoms of user data subjects. Therefore, it might also raise concern among users, although less severe in comparison with other types of risks that cause feared events. Having said that, from the healthcare efficiency perspective, there might be certain advantages of location tracking in terms of the accuracy of the results, yet as this research is dealing with the potential problematic privacy aspects, we are of the view that with high accuracy location tracking might be quite an intrusive privacy method for digital contact tracing activities. This type of concern is not commonly highlighted by scholars and European data controllers, but it is still a valid risk since it is set out under the GDPR. Furthermore, this inaccurate data could inform wrong users, thereby causing false positives, which would give a rise to the term used by the study of Cho and colleagues, namely privacy from contacts. The reason being is the term "contact" refers to any individual with whom a user has exchanged tokens in a contact tracing app based on some measure of physical proximity.³³² Achieving privacy from contacts is more challenging because it is necessary to disclose whether one of the user's contacts has been diagnosed with COVID-19, thus requiring

³³⁰ Mbunge, Elliot (2020) "Integrating emerging technologies ..." op.cit., p.1634.

³³¹ See article 5-1-d of the GDPR, principles relating to processing of personal data, accuracy.

³³² Cho, Hyunghoon; Ippolito, Daphne and Yu, Yun William (2020) "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs", *arXiv preprint arXiv:2003.11511*, pp.1-12, p.3.

some information to be revealed.³³³ Hence, to correlate these two risks, inaccurate proximity data of data subjects would potentially increase the inevitable risk of revealing the wrong person's identity to other, which would create unintended disclosure of identity in the end.

Finally, there is an indirect risk of data breaches associated with the localization data of the users. In other words, revealing data subjects' location is not only causing direct risks but also indirect risks, such as identification of recently visited places. Such data might tell you, for a given area in a city, how many people traveled to that area during each hour in previous month.³³⁴ This risk is defined as "aggregated data risk", which corresponds to the fact that even if contact tracing apps do not collect precise location data, they may still collect and share aggregated location data. This data is often used for analysis and research purposes, but it can also be a privacy risk if it is not properly protected.³³⁵ For example, this information can be used to infer an individual's habits and routines, which can still be a privacy risk. Similarly, further brainstorming on the real use case scenarios, such collected data on the proximity could somehow be associated with the activities of other people in the surrounding at the time. More specifically, as per Li and colleagues' research on certain different app designs³³⁶, tech-savvy firms can also identify the precise identities of nearby diagnosed users.³³⁷ Hence, individual living in

³³³ *Ibid.*

³³⁴ Hoffman-Andrews, Jacob, and Crocker, Andrew (2020) "How to protect Privacy When Aggregating Location Data Fight Covid-19", Electronic Frontier Foundation <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed on 22 June 2024)

³³⁵ Oliver, Nuria; Lepri, Bruno; Sterly, Harald; Lambiotte, Renaud; Deletaille, Sébastien; De Nadai, Marco; Letouzé, Emmanuel et al. (2020). "Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle", *Science advances*, vol. 6, n.23, eabc0764, pp.1-6, p.5.

³³⁶ For the full discussion on the different app designs and their ability to reveal certain info to tech-savvy users see Li, T., Faklaris, C., King, J., Agarwal, Y., Dabbish, L., & Hong, J. I. (2020) "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps", *arXiv preprint arXiv:2005.11957*.

³³⁷ *Ibid.*, p.3.

society might rightly not want to be traced once they are participating in privacy sensitive events (e.g., political demonstrations).³³⁸

Or differently, there are certain methods that build re-identification techniques into the aggregation itself.³³⁹ Likewise, as a further concerning news on this bit, it is impossible to completely anonymize location data, even when it has been de-identified; geographic coordinate pathways can be compared to those in other public databases to produce probabilistic models of whom they belong³⁴⁰, as also detailed under the anonymization section of this chapter. Accordingly, this is the reason why, from the risk perspective, Bluetooth based applications are generally seen as less invasive.³⁴¹ However, we must also highlight the fact that there are certain bad news on the less intrusiveness of Bluetooth based processing as well. To be more specific, it is worth noting that many risks are created by Bluetooth technology as well. There also many scholars, who still concerns often regarding the Bluetooth technology utilized by the API, as it operates inconspicuously in the background, leaving users unaware or uncertain about the specifics of their data handling,³⁴² which we believe is particularly concerning for location data given the nature of processing activities. More detail on that, first of all, anonymous data processing also exposes the identity of the contacting citizen on the other side. Although these data are kept anonymous as names, the issue of where the collected data will be recorded and how long it will be recorded is another issue that attracts attention. The main reason for this is that the collected data is collected from everyone's own device and then deleted without allowing the data subjects to be recognized without pairing them with anyone over Bluetooth. Furthermore, integrating the contact tracing function into the

³³⁸ Joseph K. Liu; Man Ho Au; Tsz Hon Yuen; Cong Zuo; Jiawei Wang; Amin Sakzad; Xiapu Luo; Li Li; Kim-Kwang Raymond Choo (2021) "Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach", pp.1-26, p.2.

³³⁹ Arbuckle, Luk (2020) "Aggregated Data Provides a False Sense of Security", IAPP <https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/> (accessed on 22 June 2024)

³⁴⁰ Kleinman, Robert A., and Merkel, Colin (2020) "Digital contact tracing... ", *op. cit.*, p.654.

³⁴¹ Sharon, Tamar (2021) "Blind-sided by privacy?" *op.cit.*, p.47.

³⁴² Sharon, Tamar (2021) "Blind-sided by privacy? ", *op.cit.*, p.48.

operating system layer creates a risk of latent mass surveillance, as it places control over contact tracing microdata in the hands of Apple/Google.³⁴³ Similarly, also as per the study of Vaudenay, It is quite surprising that decentralization poses further data privacy risks than it resolves.³⁴⁴ Anonymous reports of sick individuals can be deanonymized, private encounters can be uncovered, and people may be pressured into disclosing their personal data.³⁴⁵

Within this respect, It is fair to state that breaches of personal data in digital contact tracing tools could result in unprecedented security incidents. Under the GDPR, such breaches encompass situations where compromised security leads to the unlawful or accidental destruction, alteration, loss, unauthorized disclosure of, or access to, personal data that is stored, transmitted or otherwise processed.³⁴⁶ For instance, discovering the most favorite places, secondary home addresses, addresses of the users' partners, friends, secret hobbies and etc., could be subject to indirect risks resulting from the localization feature. Although it is not easy to categorize them under a typical data breach, it might even cause more serious damage to the privacy of users and the people in their surroundings. What is more challenging is that relying on Bluetooth processing of location data is not entirely free from this type of risk itself. Although the Bluetooth model relies on the exchange of anonymous identifiers between devices to determine if two individuals have been near one another³⁴⁷, as detailed in Chapter 1, thereby not directly revealing location data, it also can still reveal information about the movements and interactions of individuals, which could be used to infer their location and other sensitive information, as described herein. For example,

³⁴³ Sharon, Tamar (2021) "Blind-sided by privacy? ", op.cit., p.48.

³⁴⁴ Vaudenay, Serge (2020) "Analysis of DP3t-between scylla and charybdis", op.cit., p.12.

³⁴⁵ Vaudenay, Serge (2020) "Analysis of dp3t-between scylla and charybdis." op.cit., p.12.

³⁴⁶ Article 4 -12 of the GDPR.

³⁴⁷ European Digital Rights (EDRi). (2020) "Bluetooth-based contact tracing: What you need to know" <https://edri.org/bluetooth-based-contact-tracing-what-you-need-to-know/> (accessed on 5 February 2023).

some contact tracing apps use network analysis to identify potential infection clusters. Certainly, if an adversary can ascertain that a specific individual was the sole male visitor to a hospital clinic on a Thursday afternoon, an aggregated response to the query about "diagnoses of men who visited the clinic Thursday afternoon" could expose sensitive information directly linked to that individual's identity.³⁴⁸ Therefore, any aforementioned unauthorized surveillance of the actual location of users would constitute a serious concern for the data subjects' personal life details, regardless of the processing method, considering that indirect means of privacy intrusiveness are also as hazardous as direct breaches. It would be the most concerning cause for the European data controllers of the applications, as most of them are relying on non-GPS solutions, as detailed in Chapter 1. Therefore, such risk is still viable for European contact tracing applications, and it will be addressed in Chapter 3.

Hence, in summary, it is fair to state that the number of risks related to location data associated with using contact tracing applications can reach countless levels. The reason is like that explained in the first section due to the novelty of the applications; naturally, we can witness the type of concerns and risks related to using the applications we have never seen. To this end, to mitigate these newly emerging risks in the field of privacy law, tailor-made regulatory solutions for such cutting-edge risks related to the processing of location data will be addressed in Chapter 3 and 4 under the GDPR.

3. Architecture Risks

As briefly introduced earlier in Chapter 1, one of the most controversial aspects of contact tracing applications is their architectural design. The main reason of this is to ongoing access of authorities to personal data of users stored in central repository. This is why, applications adopting a centralized tracking approach have faced significant criticisms from human rights

³⁴⁸ Ohm, Paul (2009) "Broken promises of privacy: Responding to the surprising failure of anonymization." *UCLA L. Rev.* 57, p.1701.

organizations and the security community.³⁴⁹ However, it does not necessarily mean that one selected architecture would be entirely free from these risks either. In other words, both Bluetooth and anonymous data processing, or location data processing via GPS, cause certain risks and vulnerabilities in data protection and intrusiveness as touched in the previous section. Therefore, we believe that we cannot simply interpret architecture related risks in isolation of processing technologies selected by the controllers, due to the interplay between them. Accordingly, various models of centralized, partially centralized, or decentralized architectures do exist, yet any of them do not completely avoid vulnerabilities and risks of reidentification of personal data processed either, since, as seen, the risk is not only resulting from the architectural choice of data controllers. However, for sure, it also has a complementary impact in the re-identification risks generated by Bluetooth and GPS. In more detail, the privacy risk, by its nature, for infected users is identically to the centralized model in the GPS based model³⁵⁰. Similarly to the centralized model in the GPS based system, users have no choice but to trust the authorities will keep their information safe and private.³⁵¹ As also detailed in GPS section that the most well-known one is that the data in the centralized system increases the power of governments to monitor citizens.³⁵² This is fundamentally correct, and causes a certain degree of risk on the privacy of data subjects. Hence, centralized apps are exposed to intense privacy risk, since fundamentally the central servers request users' personal identifiable information (e.g., phone number, name, postcode, or even

³⁴⁹ Huang, Jianwei; Yegneswaran, Vinod; Porras, Phillip and Gu, Guofei (2020) "On the privacy and integrity risks of contact-tracing applications", *arXiv preprint arXiv:2012.03283*, pp.1-17, p.1.

³⁵⁰ Wang, Dong, and Fang Liu. (2020) "Privacy Risk and Preservation in Contact Tracing of COVID-19." *Chance* 33, no. 3 pp.49-55, p.53.

³⁵¹ *Ibid.*

³⁵² See Duke TechPolicy Sanford Article (2021) "Comparing centralized and decentralized contact-tracing approaches" available at: <https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/> (accessed on 17 March 2024).

location information) during registration or execution).³⁵³ This sub-component of centralized architecture is not a typical data protection concern linked with surveillance but is related to the identification of the users by a central authority. It means that it could be even more detrimental from the privacy-first perspective, as users would be subject to further anti-privacy-friendly behaviors, such as linking each personal data collected about the user from different channels of governments with the existing data processed by centralized servers.

To be more specific, governments, or application developers can acquire de-identified data on proximity and infection through centralized data systems, which have the advantage of enabling modeling and analytics to understand better the disease and also its spread.³⁵⁴ Although the users could turn off the processing of any sort of unnecessary information related to themselves when they are not in contact with any other individual,³⁵⁵ it is still risky to be subject to such modeling that might cause the re-identification of the data processed as it is stored in centralized repository. Due to this reason, many scholars from the risk-based perspective, considered the decentralized approach is more privacy-friendly since information on the infected users' close contacts is not accessible centrally by the relevant authorities,³⁵⁶ rather they are stored in the users' mobile phone. Accordingly, it could, not only have various data leakages, but also in the meantime, the identity of an infected user could be

³⁵³ Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth; Camtepe, Seyit and Ranasinghe, Damith C. (2021) "An empirical assessment of global COVID-19 contact tracing applications", *IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, pp. 1085-1097, p.1092.

³⁵⁴ Scassa, Teresa; Millar, Jason and Bronson, Kelly (2020) "Privacy, Ethics, and Contact-tracing Apps", in Colleen M. Flood, Vanessa MacDonnell, Jane Philpott, Sophie Thériault and Sridhar Venkatapuram, eds., *Vulnerable: The Law and Policy of COVID-19*, University of Ottawa Press, pp.1-8, p.3.

³⁵⁵ Samuel, Gabby; Roberts, Stephen L.; Fiske, Amelia; Lucivero Federica; McLennan, Stuart; Phillips, Amicia; Hayes, Sarah and Johnson, Suzanne B. (2022) "COVID-19 contact tracing apps: UK public perceptions." *Critical Public Health*, vol.32, no. 1, pp.31-43, p.33.

³⁵⁶ See Office of Privacy Commissioner for Personal Data, Hong Kong (PCPD), Data privacy issues relating to COVID-19 contact tracing apps. https://www.pcpd.org.hk/english/news_events/newspaper/newspaper_20210329.html (accessed on 23 June 2024).

de-anonymized by authorities or other users,³⁵⁷ as discussed. For instance, If the central server is compromised or the overseeing body misuses the information, it could identify phones and their owners by linking them to specific temporary IDs, leading to privacy risks such as identifying infected individuals and mapping a user's social circle.³⁵⁸

That being said on the risks generated by centralized storage, it is also important to understand that decentralized architecture is not completely free of privacy and security concerns either, yet, actually opens apps based on these APIs to novel and uncharted classes of privacy and security vulnerabilities.³⁵⁹ For example, because these contact-tracing systems reveal health status in connection with a unique (if rotating) identifier, it is possible to correlate infected people with their pictures using a stationary camera connected to a Bluetooth device in a public place.³⁶⁰ Accordingly, to mitigate this risk, which is not subject to further investigation in the existing literature, the EPDB took an action and provided the idea that data broadcasted through applications must merely contain some pseudonymous and unique identifiers specific to the apps.³⁶¹ By this, as per their reasoning, the potential match of identifiers that would cause revealing identities of users would directly be mitigated in its source,³⁶² whose details are to be discussed in the following chapters as one of the potential solutions to mitigate such risks.

³⁵⁷ Sowmiya B, Abhijith VS, Sudersan S, Sakthi Jaya Sundar R, Thangavel M, Varalakshmi P. A (2021) "Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19", SN Comput Sci., vol.2, n.3,136. doi: 10.1007/s42979-021-00520-z, pp.1-11, p.2.

³⁵⁸ Duke, Sanford of Public Policy, Comparing Centralized and Decentralized Contact Tracing Approaches <https://techpolicy.sanford.duke.edu/centralizedvsdecentralized/> (accessed on 3 September 2022).

³⁵⁹ Soltani, Ashkan, Calo, Ryan and Bergstrom, Carl (2020) "Contact-tracing apps are not a solution to the COVID-19 crisis." Brookings Institution. United States of America, Why Contact Tracing Could be a Disaster? <https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/> (accessed on 10 June 2024)

³⁶⁰ *ibid.*

³⁶¹ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.9.

³⁶² EDPB (2020) Guidelines 04/2020, *op. cit.*, p.9.

Additionally, within the scope of decentralized model, even though information of applications' users remains private from the central authorities, in Li and colleagues' words, "tech-savvy users"³⁶³ may have the ability to infer the identities of the diagnosed users that they have been in close proximity to³⁶⁴, which is another concern. In other words, considering that for the app to function, users are required to keep their Bluetooth Low Energy (BLE) activated continually, which opens a potential window for third parties to track these users.³⁶⁵ As such, Tech-savvy users may be able to infer the identities of some infected users they have been in contact with by logging additional location information or opening multiple accounts³⁶⁶ According to Li and colleagues' research on certain different app designs, tech-savvy individuals can also access the location history of diagnosed users in public areas with an accuracy of approximately 1000 meters (3000 feet).³⁶⁷ Obviously, all of these concerns brings another dimension to the risk definition of decentralized architecture. Moreover, we believe it is noteworthy that even in the decentralized model, there is a server that receives from the apps the notification that the app owner was tested positive, which does not need to store the association between the app owner (from which the message is coming) and his/her health state, but there is still one point in which this

³⁶³ For the full discussion on the definition see Li, Tianshi, Faklaris, Cori; King, Jennifer; Agarwal, Yuvraj; Dabbish, Laura and Hong, Jason I. (2020) "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps", *arXiv preprint arXiv:2005.11957*, pp.1-23, p.3.

³⁶⁴ Li, Tianshi, Faklaris, Cori; King, Jennifer; Agarwal, Yuvraj; Dabbish, Laura and Hong, Jason I. (2020). "Decentralized is not risk-free....", *op.cit.*, p.3.

³⁶⁵ Silvieira, Alessandra, Covelo de Abreu, Joana, Cabral, Tiago Sergio (2020) "The Mandatory Contact Tracing App StayAway Covid a Matter of EU Law", *UNIO EU Law Journal* <https://officialblogofunio.com/2020/10/20/the-mandatory-contact-tracing-app-stayaway-covid-a-matter-of-european-union-law/> (accessed on 23 June 2024).

³⁶⁶ Silvieira, Alessandra, Covelo de Abreu, Joana, Cabral, Tiago Sergio (2020) "The Mandatory Contact Tracing App StayAway Covid a Matter of EU Law", *UNIO EU Law Journal* <https://officialblogofunio.com/2020/10/20/the-mandatory-contact-tracing-app-stayaway-covid-a-matter-of-european-union-law/> (accessed on 23 June 2024).

³⁶⁷ Li, T., Faklaris, C., King, J., Agarwal, Y., Dabbish, L., & Hong, J. I. (2020). "Decentralized is not risk-free....", *op.cit.*, p.9.

information could potentially be collected.³⁶⁸ Accordingly, within this context, hackers can benefit from any vulnerabilities of decentralized model as well. More specifically, as mentioned earlier, in the decentralized approach, apps store a cache of temporary IDs they have broadcasted, while the server only holds the temporary IDs of users who have tested positive.³⁶⁹ This design sacrifices some privacy for infected users, as their temporary IDs are published by the server for all apps to verify. However, the server does not hold any information on uninfected users that could be misused. Nonetheless, since temporary IDs cannot be immediately deleted from a phone, a hacker who accesses an individual phone could learn the temporary IDs linked to the user.³⁷⁰

Therefore, considering the aforementioned risks, it is fair to state that both approaches assume a different source of user data protection risk, and both of which is applicable to European applications. While the centralized approach assumes that individual user data which could be leaked through the application is the most notable risk, the decentralized approach assumes that the compromising of all the user data in one location is the largest risk. Furthermore, Queen Mary scholars, in their research, mentioned the fact that users turned to be more concerned about their personal data, rather than the choice of centralized or decentralized architecture.³⁷¹ Hence, from our perspective, there is not any single guaranteed contact tracing architecture that would inherently be privacy-risk-free. To put it differently, both solutions appear with their advantages and disadvantages, and no consensus has been found in the privacy community, and privacy risks were determined for any of

³⁶⁸Maccari, Leonardo, and Cagno, Valeria (2021) "Do we need a contact tracing app?", *Computer Communications*, vol. 166, pp. 9-18, p.13

³⁶⁹ Duke, Sanford of Public Policy, Comparing Centralized and Decentralized Contact Tracing Approaches <https://techpolicy.sanford.duke.edu/centralizedvsdecentralized/> (accessed on 3 September 2022).

³⁷⁰ *Ibid.*

³⁷¹ Security Week, Security, Privacy Issues Found in Tens of COVID-19 Contact Tracing Apps, available at <https://www.securityweek.com/security-privacy-issues-found-tens-covid-19-contact-tracing-apps/> (accessed on 27 March 2023).

them.³⁷² By their nature, both architectures are strongly correlated with the concept of data minimization is further discussed and addressed in Chapter 3 under the data minimization section. Accordingly, the EPDB Guideline³⁷³ pointed out the significance of proportional data processing rather than pointing out one single architectural solution, which we completely agree with. According to their statement, the ongoing health crisis should not be seen as a chance to implement excessive data storage practices. The principle of storage limitation must consider genuine needs and medical relevance, which may include epidemiological factors like the incubation period. Personal data should be kept only for the duration of the COVID-19 crisis and, generally, should be deleted or anonymized once the pandemic ends.³⁷⁴ As per this statement, their approach seems to be wary of any data protection concerns that could result from the over-retention of personal data and unauthorized disclosures thereof.

The common approach is that when infected persons use privacy-preserving exposure notification applications, the identity of the establishments visited by the infected individuals when they were contagious is likewise guaranteed to be kept a secret because the location history of the infected individuals can be obscured.³⁷⁵ The exposed individuals do not need to reveal their location information until they get tested and are found to be infected also. However, at the same time, the risks associated with the places visited by the user remain viable, following the positive test results. In other words, infected people can be under the surveillance of data controllers to notify uninfected people within the surrounding. Although various practices are currently being implemented by data controllers to mitigate such inherent risks, it is still possible to encounter such side effects by any architecture regardless of

³⁷² Boutet, Antoine; Castelluccia, Claude; Cunche, Mathieu; Lauradou, Cédric; Roca, Vincent; Baud, Adrien and Raverdy, Pierre-Guillaume (2022) "DESIRE: Leveraging the best of centralized and decentralized contact tracing systems." *Digital Threats: Research and Practice (DTRAP)*, vol. 3, no. 3, pp.1-20, p.2.

³⁷³ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.9.

³⁷⁴ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.8.

³⁷⁵ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.8.

centralized or decentralized, which relies on the exact location and other identifiable personal data processing.

From our perspective, the study of Prabhakar and colleagues on biometric systems and privacy³⁷⁶ is quite helpful in this regard. We agree with his reasoning that stipulates many users will undoubtedly be reluctant to supply either raw or processed biometric measures to centralized applications and to dubious applications which might share the information with the other applications until we come to an agreement on the correct limitations to biometrics use.³⁷⁷ We believe, however, due to the close connection of both processing activities, their reasoning could be reflected in contact tracing risk perception of the user data subjects. As a result, the exposed or affected persons could obtain identity privacy using the app without having to reveal their identities.³⁷⁸ The underlying reason is that people are alerted more than ever to keep themselves safe from Covid 19 pandemic, and this situation, thus, may lead to a panic atmosphere in society. Thus, as a fundamental principle of public law, it is strictly unfair to benefit from such a panic atmosphere, and many people, based on our experience with our surroundings, experienced a such concern. As for achieving a high acceptance rate, considering that while digital contact tracing applications for Covid-19 provide a quicker method to trace a user's chance of contact with infected people and guide them for further actions, its effectiveness largely relies on a vast amount of the population installing the application.³⁷⁹ From our perspective, the true engine behind this aim is to mitigate any potential fear of privacy intrusion and data security matters, in particular pertaining to the choice of data architecture, as most of the debates related to detrimental

³⁷⁶ For their full study on biometric recognition, see Prabhakar, Salil; Pankanti, Sharath and Jain, Anil K. (2003) "Biometric recognition: Security and privacy concerns." *IEEE security & privacy* 1, no. 2, pp. 33-42.

³⁷⁷ Prabhakar, Salil; Pankanti, Sharath and Jain, Anil K. (2003) "Biometric recognition....", *op.cit.*, p.41.

³⁷⁸ Raskar, Ramesh; Dhillon, Ranu; Kapa, Suraj; Pahwa, Deepti; Falgas, Renaud; Sinha, Lagnojita; Prasad, Aarathi et al. (2020) "Comparing manual contact tracing.....", *op. cit.*, p.6.

³⁷⁹ Chopdar, Prasanta Kr (2022) "Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderator", *Health Policy Technol. Sep, vol.11, n.3,100651, pp.1-13, p.9.*

side effects of these apps is scattered around the choice of architecture, as elaborated and recommended in Chapter 3, 4 and 5.

Accordingly, in relation to the processing risks of the applications, C.Troncoso, who is leader of the Decentralized Privacy-Preserving Proximity Tracing project within the Pan-European Privacy-Preserving Proximity Tracing initiative, stated the decentralized approach was built with a big effort to make the server powerless, suggesting to the approach using Bluetooth tracking that does not require personal data and leaves no trail back to users.³⁸⁰ We, however, still keep our position and reiterate that both options for the architectural design of the applications pose a certain amount of inherent risk unless the mitigating steps detailed in Chapter 3 and 4 are implemented thoroughly. Hence, to summarize, there are plenty of discussions scattered around the choice of the architectural design of the apps related to data minimization, purpose limitation, and privacy by design/default notions of the GDPR. Nonetheless, potential risk mitigation actions related to risks and concerns resulting from the architecture of the applications must be addressed in Chapters 3, 4, and 5 considering the GDPR and the related European guidance, as the topic itself requires an elaborate examination of data controllers' practice.

4. Pseudonymization and Anonymization Risks

From a general perspective, pseudonymized and anonymized processing predominantly take precedence over processing activities without such technical and organizational measures, and it is a relieving measure of data protection risks at the outset of the processing activities. The most fundamental reason is that the GDPR deems the privacy-enhancing artefacts of these techniques by providing exceptions to many of the most burdensome

³⁸⁰ Duball, Joe (2020), "Centralized vs Decentralized Contact Tracing", IAPP Publications, <https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/> (accessed on 12 June 2024)

articles of the regulation once actions are taken to de-identify personal data.³⁸¹ However, within the scope of contact tracing activities, anonymous data processing may also expose the identity of the contacting citizen on the other side, thereby the re-identification of anonymized data is highly possible in our era. In other words, as stated by Tran and Nguyen, anonymity does not equate to privacy.³⁸² The reason is clever adversaries might re-identify or de-anonymize the people hidden in an anonymized database.³⁸³ In other words, the collected data is collected from everyone's own device and then deleted without allowing the data subjects to be recognized without pairing them with anyone over Bluetooth. However, it may be easier to determine who belongs to the data collected via GPS or a different technology. Where the point of discussion scatters is whether the collected data would be stored rather than how long it would be stored, whether it would be pseudonymized or anonymized after the storage period, or whether it would be deleted in a way that cannot be fully recovered from the system database. In the ideal world, although anonymization seems to be one of the safest options for privacy practices³⁸⁴, as mentioned, the point that today's technology has reached must be considered. In other words, in reality, it might be challenging to identify whether data has been appropriately anonymized or if it still contains personal information.³⁸⁵ This is mainly due to the risk-based nature of anonymization and its reliance on a number of challenging-to-quantify

³⁸¹ Wes, Matt (2020) "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization", IAPP <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/> (accessed on 22 June 2024)

³⁸² Tran, Cong Duc and Nguyen, Tin Trung (2021) "Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps", *Technology in Society*, vol. 67, 101755, pp.1-11, doi: 10.1016/j.techsoc.2021.101755. Epub 2021 Sep 21. PMID: 34566204; PMCID: PMC8454194, p.7.

³⁸³ Ohm, Paul (2009) "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA L. Rev.*, vol. 57, p.1701.

³⁸⁴ Lubowicka, Karolina (2024) "The Ultimate Guide to Data Anonymization in Analytics", PiwikPro <https://piwik.pro/blog/the-ultimate-guide-to-data-anonymization-in-analytics/> (accessed on 22 June 2024).

³⁸⁵ Esayas, Samson (2015) "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach." *European Journal of Law and Technology*, vol.6, no. 2, pp. 1-23, p.3.

elements.³⁸⁶ More particularly, this ties to the challenge of anticipating the information and technology that might be used for re-identification, thereby anonymized data being used for `re-identify` in the future.

Therefore, to apply a “zero-risk” policy, the anonymized and pseudonymized data must comply with certain requirements, as detailed in Chapter 3 and 4. Failure to comply with these requirements causes a significant data protection risk in society. As a concrete example with respect to the significance of the risk resulting from anonymization, we can look at the case in which the EDPB rendered³⁸⁷ for Danish taxi firm Taxa that efficient data anonymization is consisting of two parts:

- Being irreversible.
- Implemented in a manner that renders the data subject identification impossible or highly impractical.

As seen, there is a strong emphasis put by EDPB on the re-identification risk of data subject as part of anonymization and pseudonymization activities. Within the similar context, in Article 29 Working Party document, the Working Party analyzed different methods of data anonymization and elaborated on the required measures data processors and controllers must implement.³⁸⁸ The Working Party specifically stated that merely eliminating explicit identifying elements does not inherently guarantee the anonymity or prevention of data subject identification³⁸⁹, considering the risk posed by technological developments. Their approach is valid for our thesis as well, given that this situation entails a serious source of concern for data subjects. Otherwise, it is vastly probable to encounter feared events in terms of the re-

³⁸⁶ Esayas, Samson (2015) "The role of anonymisation and pseudonymisation ...", *op.cit.*, p.3.

³⁸⁷ See European Commission, Danish Data Protection Agency Proposes 12 DKK Million Fine https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en (accessed on 23 June 2024).

³⁸⁸ Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymization Techniques. Adopted on 10 April 2014 (wp216), p.28.

³⁸⁹ *Ibid.*

identification of personal data processed, which causes a massive data protection risk under the GDPR. Moreover, referring back to the above mentioned Taxa a Danish taxi company case, it has not deleted or anonymized the data it has previously collected from the drivers, within the time stipulated in GDPR.³⁹⁰ As such, the company was severely punished by the European Commission in the end. The fundamental reason for this penalty is that the Taxa company, which works through an application with the logic of uber, claims that it carries out the process of anonymizing the data subject of its customers by simply deleting their names. However, the anonymized data could still be associated with the data subject passengers at the time. Hence, we are of view that the same data protection risk detailed in the case may also arise within the scope of contact tracing applications, as mentioned. That being said, we are not claiming that there is huge likelihood of data subjects being identified by third parties easily, even if data is anonymized. However, from our perspective, there is always risk of re-identification of data subject, considering that proper anonymization methodology referred by WP29³⁹¹ is a costly and sometimes error-prone concept, as in the case of Taxa company as well. Therefore, to be more specific on the reasoning of such re-identification risk, we can provide that although contact tracing systems do not explicitly collect or record the true identities of individual users, movement profiles based on pseudonymous tracing data, a considerable percentage of users can still be positively identified.³⁹² This is mainly because movement profiles of the users are quite distinctive,³⁹³ which, thus, we believe

³⁹⁰See European Commission Website, Danish Data Protection Agency Proposes 12 DKK Million Fine https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en (accessed on 23 June 2024)

³⁹¹ Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymization Techniques. *op.cit.* p.9.

³⁹² Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira et al. (2020) "Mind the gap: Security & privacy risks of contact tracing apps", *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, pp. 458-467, p.461.

³⁹³ Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira et al.. (2020) "Mind the gap: Security & privacy risks...", *op.cit.*, p.461.

that pseudonymous identifiers can still pinpoint the relevant data subjects in light of contact tracing applications' approach. Even by itself, we are of view that, this concept indicates that there is a risk of identification of data subjects' certain aspects, i.e., location or whereabouts, even if not all the personal details due to the pseudonymized nature of data. Having said that, we are not aiming to advocate for constant skepticism about enhanced identification methodologies of data subjects' anonymized or pseudonymized data, but rather we are trying to indicate that unique nature of contact tracing applications could have different implications on identification risks.

As such, within the same remit, several other possibilities for de-anonymization risk on data subjects have also been proposed in the existing literature for the risks generated by de-anonymization. For example, by placing a Bluetooth LE sensor close to a camera with facial recognition functionality, it is, in principle, possible to directly associate the proximity identifier beamed over Bluetooth LE (and thus the used pseudonym) with an identifiable person to entirely de-anonymize the person in question.³⁹⁴ Similarly, within the same remit, knowing the social graphs of a significant number of users can be further used to de-anonymize these users.³⁹⁵ For instance, in case an attacker has access to side-channel information, such as online social networks, he can match it to the global social graph he has reconstructed with contact tracing and then re-identify the users in this graph.³⁹⁶ Likewise, an eavesdropper can also identify a user as positive for the disease, by cross-referencing the "infected" beacons published by the authorities with the beacons acquired via eavesdropping. The same data may also allow an adversary to track the locations that a positively diagnosed

³⁹⁴ Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira et al. (2020) "Mind the gap: Security & privacy risks...", *op.cit.*, p.461.

³⁹⁵ Bobbio, Andrea; Campanile, Lelio; Gribaudo, Marco; Iacono, Mauro; Marulli, Fiammetta and Mastroianni, Michele (2023) "A cyber warfare perspective on risks related to health IoT devices and contact tracing." *Neural Computing and Applications*, vol. 35, no. 19, pp. 13823-13837, p.13823.

³⁹⁶ Bobbio, Andrea, Lelio Campanile, Marco Gribaudo, Mauro Iacono, Fiammetta Marulli, and Michele Mastroianni. (2022) "A cyber warfare perspective...", *op. cit.*, p.13823.

individual has visited.³⁹⁷ Therefore, as seen, there are multiple innovative way of accomplishing de-anonymization of data at stake, which is unfortunately scary but highly possible.

That being said, we believe using anonymized data for statistical purposes is appealing for controllers to apply anonymization techniques on collected data, rather than delete them irreversibly. For example, as detailed in Chapter 1, some countries, including but not limited to, Austria³⁹⁸ Czechia³⁹⁹ and Germany⁴⁰⁰ are reliant on this statistical purpose of processing for their digital contact tracing activities. This, inevitably, might create a basis for such inherent risks on the data subjects due to the above-mentioned enhanced capabilities of re-identification of data subject. Accordingly, the UK Information Commissioner's Office (hereinafter referred to as "ICO")⁴⁰¹ provided detailed information around the potential risks resulted from general practices of controllers for anonymizing data instead of deleting it, which we believe is applicable to the data controllers of contact tracing application in EEA/EU, considering that retaining anonymized data for statistical analysis is associated with similar concerns on other controllers. In more detail,

³⁹⁷ *Ibid.*

³⁹⁸ Stopp Corona Application, privacy policy, op.cit. Section 4.9.

³⁹⁹ eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, op.cit., Section "Who has access to your data", p.13.

⁴⁰⁰ Corona Warn, Privacy Notice, op.cit., Section 5-1.

⁴⁰¹ In the course of our work, we also utilized the ICO's guidelines when necessary. This was due to the fact that both the EDPB and the ICO frequently reference each other's guidelines as additional information sources, given the similarities in data protection regulations outlined by the ICO. As stated by the ICO, the EU GDPR's provisions have been directly incorporated into UK law as the UK GDPR, resulting in minimal changes to the core data protection principles, rights, and obligations. GDPR recitals provide additional context and help elucidate the binding articles. These recitals maintain their previous status—they are not legally binding but are valuable for interpreting the articles. For the further information see <https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/> (accessed on 27 June 2024).

Information Commissioner's Office ("ICO") listed⁴⁰² the following risk types on anonymization practices in general:

- Assessing the risk of re-identification with absolute certainty can be impossible.
- Many situations will require careful judgment based on the specific circumstances.
- If controllers generate personal data through a re-identification process, controllers will assume data controller responsibilities.

Hence, in light of the existence such material inherent risks, and drastic responsibilities attributed to the controllers, even though his statistical purpose seems to be one of the most needed inputs for data controllers, which, as said, might have indirect impact on the re-identification of the data subjects in the end, which will be later detailed in this thesis in the following chapters.

Overall, it is fair to state that there is a risk of re-identification of data subjects' anonymized and pseudonymized data generated by the advanced techniques and methodologies described herein. Moreover, type of methods to reidentify anonymized or pseudonymized data will probably keep being varied day by day, given that the tracking technologies are now reaching another level. As a key takeaway, it is not possible to cover all existing technologies for the re-identification of data subjects in single research, but we would like to reiterate that each data controller and application developer must always be alerted regarding the presence of such evolving and growing risks. To this end, the mitigation of these risks by controllers will be addressed in Chapter 3 and 4 under the existing European regulations and guidance.

5. Data Storage and Management Risks

⁴⁰² Information Commissioner's Office (2012) "Anonymisation: managing data protection risk code of practice." ICO, available at: <https://ico.org.uk/media/1061/anonymisation-code.pdf>, p.18.

As introduced in the first chapter, data protection and the application of fair information practices aim to responsibly manage and utilize individuals' information, mitigating potential risks associated with data and its usage.⁴⁰³ They encourage data practices that protect information against misappropriation, loss, or misuse and that ultimately protect individuals from the harm that may result.⁴⁰⁴ The reason being is, in general, for any apps, there are many access points for an outside actor to take advantage of in an industrial environment where thousands of sensors and other linked devices have been deployed.⁴⁰⁵ The risk of being subjected to cyberattacks increases as industrial environments become more digitalized.⁴⁰⁶ Thus, returning to the focus of our research, we emphasize that using contact tracing apps necessitates gathering significant amounts of personal information, such as names, phone numbers, and health data, which may be susceptible to misuse and hacking. Consequently, concerns about data collection, usage, and security are increasing.⁴⁰⁷ Nonetheless, for contact tracing applications to automatically alert potential contacts who might have meet the infected person while they were contagious due to their close proximity to the infected person, the infected person must disclose their location history. Therefore, many contact tracing apps lack adequate data protections, such as strong encryption and secure data storage, which can increase the risk of data protection violations. For instance, information handling in a centralized system is vulnerable to manipulation and corruption.⁴⁰⁸ In addition, any digital contact tracking system's central server may have access to the user's

⁴⁰³ Krasnow Waterman, Karen, and Bruening, Paula J. (2014) "Big Data analytics: risks and responsibilities", *International Data Privacy Law*, vol.4, no. 2, pp. 89-95, p.89.

⁴⁰⁴ Krasnow Waterman, Karen, and Bruening, Paula J. (2014) "Big Data analytics...", *op.cit.*, p.89.

⁴⁰⁵ Paez, Mauricio and Tobitsch, Kerianne (2017) "The industrial internet of things: Risks, liabilities, and emerging legal issues", *NYL Sch. L. Rev.*, vol.62, pp.217-247, p.221.

⁴⁰⁶ Paez, Mauricio and Tobitsch, Kerianne (2017) "The industrial internet of things...", *op.cit.*, p.221.

⁴⁰⁷ Sowmiya, B., V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi (2021) "A survey on security and privacy....." *op.cit.*, p.2.

⁴⁰⁸ Sowmiya, B., V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi (2021) "A survey on security and privacy....." *op.cit.*, p.2.

personal or personally identifiable information i.e., phone number, postal code, and so forth. Likewise, there is also a significant risk of losing users' data privacy in case these datasets are not saved in an encrypted format.⁴⁰⁹ Accordingly, in 2020, it was reported that the personal information of millions of users of the Corona 100m app was leaked, potentially exposing sensitive information to cybercriminals.⁴¹⁰ Therefore, retaining this many data in a single center, will not only cause a breach of data protection laws, but also increase the risk of cyber-attack or leakage.

Accordingly, for the efficient analyze of the situation at stake, we are of view that it is crucial to understand the nuances of cyberattacks, as it is closely connected with these discussions. To be more specific, with regards to cyber-attacks on the personal data collected, Chan and colleagues provided insight into attacks, and discussed three functionalities on best harness computing technologies to support the goals of public health agencies to reduce Covid related morbidity and mortality while defending individuals' civil liberties, four categories are in jeopardy.⁴¹¹ It is significant to determine these questions about the potential for malicious hackers, governments, or organizations to compromise the system, because of such attacks, a privacy maximalist would be justified in not using any decentralized automated contact tracing systems.⁴¹² Accordingly, Chan and colleagues⁴¹³ indicated their classification

⁴⁰⁹ Chakraborty, Pranab; Maitra, Subhamoy; Nandi, Mridul and Talnikar, Suprita (2020) "Contact Tracing in Post-Covid World: A Cryptologic Approach" Singapore: Springer, pp.1-134, p.31.

⁴¹⁰ BBC News Website <https://www.bbc.com/news/world-asia-53211350> (accessed on 23 August 2022).

⁴¹¹ For the full study see Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing." *arXiv preprint arXiv:2004.03544*, PPR:PPR268538, pp.1-22.

⁴¹² Bengio, Yoshua; Ippolito, Daphne; Janda, Richard; Jarvie, Max; Prud'homme, Benjamin; Rousseau, Jean-François; Sharma, Abhinav and Yu, Yun William (2021) "Inherent privacy limitations of decentralized contact tracing apps." *Journal of the American Medical Informatics Association*, vol. 28, no. 1 pp. 193-195, p.194.

⁴¹³ Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols..." ,*op.cit.*, p.5.

of attacks and their way of indicating their underlying logic by directing questions to data subjects as follows:

- Integrity Attacks: can a malicious person listen to your phone's broadcasts if you are negative and then report positive while posing as you?
- Inferential Attacks: can others infer where a positive citizen who decides to declare being positive is located?
- Replay and Reliability Attacks; is it feasible that a citizen who is warned that they are in danger was not near a supportive person?
- Physical Attacks: what data is exposed if a citizen's device is taken by an authority, exploited by a hacker, or stolen? ⁴¹⁴

From our perspective, all of these questions pertaining to the attacks equally are important to ask to determine any vulnerabilities of the applications and security risks related thereto. That being said it is important to highlight that the type of attacks resulted from data management of contact tracing applications are not limited to these. In other words, there are also different types of security attacks available in the literature. In more detail, there is a Blue snarfing attack, which is a security attack that forcibly connects to a Bluetooth-enabled device to access sensitive information like pictures, videos, emails, contact lists, calendars, and the International Mobile Equipment Identity (IMEI) stored in the device's memory.⁴¹⁵ The IMEI, a 15-digit unique identifier for devices, can be exploited by an attacker to redirect all incoming calls from the user's device to their own. Likewise, a playback attack, also known as a replay attack, involves delaying or maliciously repeating data transmission.⁴¹⁶ The attacker intercepts and retransmits the data, potentially as part of a masquerade attack through packet substitution. In these attacks,

⁴¹⁴ De Montjoye, Yves-Alexandre, Tarun Ramadorai, Tommaso Valtetti, and Ansgar Walther (2021) "Privacy, adoption, and truthful reporting: a simple theory of contact tracing applications", *Economics Letters*, vol. 198, pp. 109676.

⁴¹⁵ Sowmiya, B., V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi (2021) "A survey on security and privacy....." op.cit., p.6.

⁴¹⁶ Sowmiya, B., V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi (2021) "A survey on security and privacy....." op.cit., p.7.

the adversary aims to deceive users into storing misleading contact data, leading to false messages.⁴¹⁷ Moreover, considering their constantly evolving nature, there are also other type of attacks applicable to data storage and management activities of contact tracing apps.

Suitably, in the sense of these various attacks resulted from any applications of this sort, we believe that Huang and colleagues implemented useful research regarding the type of attacks and simulations of these attacks as well.⁴¹⁸ As per their research, the first adversarial model, known as the contact-isolation assault, proposes a privacy threat against app users that contract Covid-19 infection. It enables an attacker to set up probes that might essentially harvest the identities of infected users in public places where people gather frequently. To de-anonymize affected user devices, this assault integrates large-scale device spoofs with pool tests, device re-identification techniques, and online databases. The SafeGraph POI data and a simulation study were both used to assess the effectiveness of this assault.⁴¹⁹ The second adversary model takes advantage of a data-poisoning attack, which enables an adversary to compromise the applications' dependability and cause false positive alerts that would be extremely disruptive to any user base for contract tracing.⁴²⁰ Therefore, as seen, there huge variety of security attacks that could be resulted from the use of contact tracing applications, from technical perspective. That being said, it is important to highlight that data breaches stemming from contact tracing applications are not limited to security attacks either. In other words, there might be countless new type of personal data breach risks in different forms, as the pandemic presented a chance to hasten the advancement and uptake of cutting-edge

⁴¹⁷ *Ibid.* p.7.

⁴¹⁸ For the full article see Huang, Jianwei; Yegneswaran, Vinod; Porras, Phillip and Gu, Guofei (2020) "On the privacy and integrity risks of contact-tracing applications." arXiv preprint arXiv:2012.03283, pp.1-17, p.3.

⁴¹⁹ Huang, Jianwei; Yegneswaran, Vinod; Porras, Phillip and Gu, Guofei (2020) "On the privacy and integrity risks..." op.cit., p.3.

⁴²⁰ *Ibid.*

technologies,⁴²¹ thereby new types of data breaches by different actors. For instance, as detailed by the study of Shukla and colleagues, it is possible to implement such threat actors can vary from application developer, internet provider, other applications on the user device, governments and etc.⁴²²

Hence, our assessment on the main reason thereof, is due to the hurried nature of their deployment, these applications run the risk of creating unfavorable stakeholder dynamics and power imbalances as stakeholder obligations for data governance remain even after the pandemic time.⁴²³ In addition to this fact, another risk multiplier is the nature of the data at stake. To be more concrete, hackers are probably more motivated to leak users' data due to its significance. For instance, if we take medical data as a sample, given that medical data is quite sensitive as it frequently contains the majority of the data that hackers seek, including credit card numbers, Social Security numbers, and bank account details, it is providing criminals with a one-stop theft technique.⁴²⁴ Using this information, fraudsters can make fraudulent identifications to purchase resalable medical supplies or medications, or they can combine a patient's number with a fake provider number and submit phony insurance claims.⁴²⁵ Hence, it also complicates the type of personal data breach which could be subject to GDPR notification. The reason is the potential distortion of personal data, as described under article 4 of the GDPR,⁴²⁶ might be a source of concern for users as a course of general data management risk. Accordingly, as indicated by Article 29 Working Party,

⁴²¹ Li, Veronica QT, Ma, Liang and Wu, Xun (2022) "COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia", *Policy and Society*, vol. 41, issue 1, pp. 1–14, <https://doi.org/10.1093/polsoc/puab019>, p.10.

⁴²² For the full details of the threat actors see Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines...", *op. cit.*, p.5-6.

⁴²³ Li, Veronica QT, Ma, Liang and Wu, Xun (2022) "COVID-19, policy change...", *op.cit.*, p.1.

⁴²⁴ Khan, Shahidullslam, and AbuSayedMd Hoque (2016) "Digital health data: a comprehensive review of privacy and security risks and some recommendations", *Computer Science Journal of Moldova*, vol.71, n.2, pp. 273-292, p.283.

⁴²⁵ *Ibid.*

⁴²⁶ See Article 4 of the GDPR, the definition of personal data breach.

determining whether there has been a confidentiality or integrity breach is comparatively obvious, whereas an availability breach might be less evident.⁴²⁷ Thus, a breach will always be deemed as an availability breach once there is permanent loss of, or destruction of, personal data,⁴²⁸ which is more in line with the spirit of data management risks related to contact tracing applications. Nonetheless, within the context of contact tracing activities, one cannot simply conclude that such confidentiality breach should be handled in isolation, as mentioned that the identifiers or components used in medical data could end up impacting availability or integrity of other data as well. Lastly, within the same vein of breaches, there are certain amount risks stemming from the interoperability acts of the European applications as well, which are predominantly scattered around data transfers. In principle, although each of these countries falls within the scope of secure countries as per the adequacy list provided by the EU Commission⁴²⁹, there are still risks in the cross-country surveillance as well as retention and destruction of the personal data processed by the EEA countries. To be more specific on this type of risk, given that the apps are tailor-made and not standardized on a global scale, each country opted for developing a contact tracing app that has its Internet of Things infrastructure, devices, APIs, and data formats leading to interoperability issues. To elaborate on the concern, interoperability issues include the diversity of networking standards and communication protocols, variations in data semantics and ontology, differences in data formats, multiple operating systems, and different programming languages, among other factors.⁴³⁰ As such, this would potentially cause a privacy risk in terms of a data breach as mentioned above, under the GDPR, due to the fact that

⁴²⁷ Article 29 Working Party (2018) "Guidelines on Personal data breach notifications under Regulation 2016", p.8.

⁴²⁸ Article 29 Working Party (2018) "Guidelines on Personal data breach notifications under Regulation 2016", p.8.

⁴²⁹ The EU Commission Website, Adequacy Decision https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,Uruguay%20as%20providing%20adequate%20protection. (accessed on 21 March 2023).

⁴³⁰ Mbunge, Elliot (2020) "Integrating emerging technologies ..." op.cit., p.1634.

such inconsistency between the systems of data controllers would inevitably result in an excessive amount of data retention, and lack of security of processing among countries, which would end up in creating legal consequences against data subjects. Thus, the appearance of Bluetooth-based applications as the essential design did by itself does not provide interoperability,⁴³¹ as there are certainly other considerations that play role in interoperability, which could also create aforementioned risks, due to different types of approaches.

Additionally, in this regard, another risk type is associated with permissions asked by contact tracing applications. To be more specific, these applications demand a massive range of permissions, including hazardous and signature permissions.⁴³² Nevertheless, in reality, only a small number of permissions are required for simple contact tracing applications.⁴³³ For example, some existing frameworks are entirely dependent on Bluetooth low-energy (BLE technology), so seeking other permissions like location, microphone, users' contact information, and so on is no longer necessary or important for delivering the intended functionality, tracing virus propagation. Accordingly, our perspective on the issue is that it might be more terrifying once the user is confronted with several types of permissions, they might feel insecure in terms of trusting their personal data. Therefore, it might negatively affect their trust in the application. Similarly, the study of Bardus and colleagues put forward that while the number and type of permissions varied across apps, it seems that indeed, certain governments exhibit a heightened interest in

⁴³¹ Marhold, Klaus, and Fell, Jan (2022) "Multi-mode standardization under extreme time-pressure—the case of COVID-19 contact-tracing apps." *R&D Management*, vol. 52, no. 2, 356-375, p.362.

⁴³² Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021) "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps." *Empirical software engineering* 26, no. 3. pp. 1-51, p.41.

⁴³³ Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021) "A privacy and security analysis...", op.cit., p.41.

amassing larger volumes of data compared to others.⁴³⁴ As such, even though the use of Bluetooth technology for contact tracing appears to be nearly universal and has been regarded as a privacy-preserving strategy, some apps include extremely intrusive authorizations or required constant internet connectivity, which may not always be available, making a real-time exposure notification challenging or impractical.⁴³⁵

In addition, these permissions may also create ambiguity about the data minimization principle implemented by data controllers of the applications, considering that users will constantly ask for varied types of permissions to utilize these applications. The reason for such potential ambiguity is that as rational human beings, when we download an application to our mobile phones, regardless of the type of such application, we as users have always been intimated about the type of additional permissions-related questions asked to ourselves. For instance, considering Norwegian application, whose use was forbidden by the Norwegian Data Protection Authority on temporary basis⁴³⁶ is a great exemplification of such situation. Norwegian authority temporarily forbidden the processing of personal data of Smittestopp app, as the Norwegian Institute of Public Health (NIPH) found that the NIPH did not sufficiently establish the necessity of using location data from GPS in contact tracing, which they find is in breach of data minimization principle.⁴³⁷ This sample, is pretty self-explanatory for the materiality of the risk at stake regarding overarching application of data minimization principle, which also valid to the risks delineated in location risks section of this chapter. Therefore, this logic behind the excessive amount of permission requests that could be

⁴³⁴ Bardus, Marco; Al Daccache, Melodie; Maalouf, Noel; Al Sarih, Rayan and Imad H. Elhaji. (2022) "Data Management and Privacy Policy of COVID-19 Contact-Tracing Apps: Systematic Review and Content Analysis", *JMIR Mhealth Uhealth*, vol. 10, n.7, e3519, pp.1-20, p.19.

⁴³⁵ *Ibid.*, p.19 and p.20.

⁴³⁶ For the full details of the decision see EDPB, Temporary suspension of the Norwegian Covid-19 contact tracing app https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en (accessed on 23 August 2022).

⁴³⁷ EDPB, Temporary suspension of the Norwegian Covid-19 contact tracing app https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en (accessed on 23 August 2022).

detrimental to the privacy-first approach might provide content for contact tracing applications as well. However, it is also worth noting what research of Raab offered in terms of privacy risks.⁴³⁸ Raab mentioned that the degree of trust or distrust had been highlighted as crucial, especially regarding perceived demands or requirements for enhanced data protection, and levels of awareness and knowledge of privacy concerns, process innovations, and the administration use of data have been determined.⁴³⁹ Accordingly, our evaluation of the situation is that obviously enhanced data protection is a key component of solidifying people's trust in any kind of digital application, including but not limited to contact tracing applications, considering that there a massive risk generated by damaging the trust of users. Even a questionnaire related to data management practices provided by a data controller of a random application plays an important role in making data subjects feel the freedom of choice between different data storage and management activities. This is certainly an important aspect associated with trust, fear, or distrust about any sort of application. It is important to understand the causes of risks related to mistrust of users, and their privacy perception at the first place from a legal and technical perspective. For instance, in a similar vein, we believe that the study of Oomen and Leenes could be a useful standpoint to understand why such distrust appears in the first place. More specifically, as they mentioned, privacy risks are regarded as the consequences of the abuse or misuse of personal information.⁴⁴⁰ Possible privacy risks can, thus, be identity theft, loss of freedom, threat to personal safety, threat to dignity, invasion of the private sphere, unjust treatment, or financial loss.⁴⁴¹ For example, the Covid exposure notification app developed by Apple and Google, known as the Exposure Notification API, collected

⁴³⁸ For the full study see Raab, Charles D. (1998) "The distribution of privacy risks: Who needs protection?", *The information society*, vol. 14, no. 4, pp. 263-274.

⁴³⁹ Raab, Charles D. (1998) "The distribution of privacy risks: Who needs protection?", *The information society*, vol.14, no. 4, pp. 263-274, p.270.

⁴⁴⁰ Oomen, Isabelle, and Leenes, Ronald (2008) "Privacy risk perceptions and privacy protection strategies", *Policies and research in identity management*, pp. 121-138. Springer, Boston, p.122.

⁴⁴¹ *Ibid.*

information such as names, phone numbers, and health status from users.⁴⁴² This information was then used to identify individuals who had been in close proximity to someone who had tested positive for COVID-19, and to send notifications to those individuals advising them to self-quarantine. However, the collection of this type of personal information could also raise data protection concerns, since it makes individuals' sensitive information vulnerable to hacking and misuse, as it was indicated in this case. Likewise, within the similar sense, as one of the concerns resulted in the same fashion could be most devices gathering an excessive amount of device information, such as the operating system and model, without clear reasons for why this data is being collected, as the study of Wen and colleagues indicated.⁴⁴³ This would be, again, concerning in the sense of breaching purpose limitation and data minimization principles in the GDPR, given that there are overarching use of the data collected. Similarly, as another example of such misuse resulted from the excessive data collection, an app called "Aarogya Setu" demanded users to provide their mobile number, name, gender, age, a list of countries they have visited in the past 30 days, and profession.⁴⁴⁴ As such, we are of view that profession, mobile phone number, gender, full name of the data subject, therefore, is quite an excessive for the contact tracing purpose. Or as another example of unnecessary collection of data, as indicated by Sowmiya and colleagues that geo-location tracking is redundant when Bluetooth or similar wireless technologies are used.⁴⁴⁵ Therefore, as seen, plenty of samples could be derived for the risk of collection excessive amount of personal data, which would automatically result in further concerns and

⁴⁴² Apple and Google (2020), The Exposure Notification API <https://developer.apple.com/documentation/exposurenotification> (accessed on 23 June 2024).

⁴⁴³ Wen, Haohuang; Zhao, Qingchuan; Lin, Zhiqiang; Xuan, Dong and Shroff, Ness (2020) "A study of the privacy of covid-19 contact tracing apps", *Security and Privacy in Communication Networks: 16th EAI International Conference, SecureComm 2020, Washington, DC, USA, October 21-23, 2020, Proceedings, Part I*, n.16, Springer International Publishing, pp. 297-317, p. 313.

⁴⁴⁴ Sowmiya, B., V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi (2021) "A survey on security and privacy issues in contact tracing application of Covid-19", *SN computer science*, vol.2, pp. 1-11, p.6.

⁴⁴⁵ Ibid., p.7.

risks, considering the prevalent approach on processing too much data on users in almost every line of activities.

Furthermore, another risk that could be associated with use of contact tracing applications is related to the identity of the application developer. To put it differently, increased outsourcing and offshoring are to blame for the rise in external security vulnerabilities. Risk rises as more people, including suppliers, intermediaries, and subcontractors, gain access to user data as security shifts from an internal and "domestic" problem to an external and "international" one.⁴⁴⁶ It is not strictly related to any offshoring relation, yet is related to any type of service or product procurement relation about digital contact tracing applications. Therefore, contrary to the risk related to governmental use of personal data in the contact tracing process, there is also a risk, which may occur for many other private initiatives, such as the GAEN initiative, the biggest concern is that the data in question has been or will be separated and used for advertising or commercial purposes in the future. Although GAEN was the product of two prestigious companies, these questions must be resolved as all possibilities are tested within the framework of contact tracing applications. Also, Australia was also receiving assistance for data storage matters from Amazon and Microsoft. There is a significant challenge with respect to security and privacy within smartphone applications is sharing data with third parties to aid targeted advertisements.⁴⁴⁷ In other words, the seamless transfer of digital data across different contexts, each governed by distinct privacy standards, contrasts with the restricted movement seen in the paper-based era and has sparked new concerns about "mission creep".⁴⁴⁸ For example, the health data gathered for contact tracing

⁴⁴⁶ Nassimbeni, Guido; Sartor, Marco and Dus, Daiana (2012) "Security risks in service offshoring and outsourcing." *Industrial Management & Data Systems* 112, no. 3, pp.405-440, p.408.

⁴⁴⁷ Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2021) "A First Look at Privacy Analysis of COVID-19 Contact-Tracing Mobile Applications," in *IEEE Internet of Things Journal*, vol. 8, no. 21, pp.15796-15806, p.15803.

⁴⁴⁸ Sharon, Tamar (2021) "Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers." *Ethics and Information Technology* 23, no. Suppl 1, pp. 45-57, p.46.

could potentially be repurposed by third parties to dictate access to work or public spaces, such as subways, malls, and markets.⁴⁴⁹ Nevertheless, although there is third-party access to personal data within the scope of using these applications, users still opt for downloading them. Smartphone applications using such strategies leverage advanced analytics techniques to identify user behavior and profiles to achieve personalized advertisements.⁴⁵⁰ Within this context, the information collected by track and trace apps is highly personalized and if made accessible to third parties can lead to sophisticated advertisement techniques breaching public trust and confidence in such apps.⁴⁵¹ As stated by the study of Xu, and colleagues, there were apprehensions regarding the NHSX-Tech company collaborations, particularly regarding the accessibility and conditions surrounding the data collected by the app.⁴⁵² There were concerns that this data could potentially feed into the NHS COVID-19 datastore, involving significant technology partners such as Google, Amazon, and Palantir.⁴⁵³ Moreover, these third-party access-related risks are not limited to what has been provided so far, as there is a risk of secondary use of such personal data collected. This type of concern was also delineated by Xu and colleagues within the scope of their studies on measuring mobile users' concern for data protection. As per the research, when a new linkage takes place without users' (i.e., data subjects') knowledge or consent, privacy concerns from users regarding the secondary use of data would be raised.⁴⁵⁴ When a vendor discloses collected personal

⁴⁴⁹ *Ibid.* p.46.

⁴⁵⁰ *Ibid.* p.47.

⁴⁵¹ Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2021) "A First Look at Privacy.....", *op.cit.*, p.15803.

⁴⁵² Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, vol.12, no. 12, 1, p.802.

⁴⁵³ Samuel, Gabby; Roberts, Stephen L.; Fiske, Amelia; Lucivero Federica; McLennan, Stuart; Phillips, Amicia; Hayes, Sarah and Johnson, Suzanne B. (2022) "COVID-19 contact tracing apps: UK public perceptions", *Critical Public Health*, vol.32, n.1, pp. 31-43, DOI: 10.1080/09581596.2021.1909707, p.33.

⁴⁵⁴ Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy...", *op.cit.* p.802.

data to unapproved parties or utilizes it for unintended secondary applications without customers' knowledge or consent, the link coordination rules are frequently seen to have been violated.⁴⁵⁵ From our perspective, this particular concern is quite valid for people opting out of downloading such applications in GDPR countries as well. We believe that concerns related to the use of personal data for commercial purposes by companies could be as exhausting sometimes due to the vast number of such companies relying on behavioral advertising in our era. Similarly, this can lead to users' location data being shared with companies that they did not explicitly authorize, which can be a significant violation of privacy. Therefore, it is fair to state that either way of surveillance is a drastic source of concern for users.

Overall, as seen, there are certain level of risk exposure generated by the data management practices of contact tracing apps in terms of data minimization, security of processing and purpose limitation principles. As indicated by the study of de Montjoye and colleagues that the extent of adoption of the apps will count on a number of variables, such as the safety of the data gathering process and the potential for adopters to receive guarantees of anonymity.⁴⁵⁶ Therefore, it is of significance to identify such concerns on data management and mitigate those concerns efficiently. As such, to have a more elaborate approach related to the mitigation of risks stemming from data storage and management of personal data, the act of data controllers will be examined in light the GDPR and other EU guidance in Chapters 3,4, and 5, and tailor-made solutions for more efficient practices will be provided.

6. Obligatory Use Risks

With regards to the principal of voluntarism regarding the use of these applications, as mentioned earlier in Chapter 1 that the global counterparts of the applications were mandated to automate contact tracing to citizens of

⁴⁵⁵ Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy...", *op.cit.* p.802.

⁴⁵⁶ de Montjoye, Yves-Alexandre, Tarun Ramadorai, Tommaso Valletti, and Ansgar Walther (2021) "Privacy, adoption, and truthful....", *op.cit.*, p. 109676.

many countries.⁴⁵⁷ As a result of such mandate, across the World, from the voluntariness perspective, these systems are found massively complex and lacking in the transparency necessary for legislators to make sufficiently informed decisions on their implementation.⁴⁵⁸ Therefore, as a natural outcome of such mandatory approach, many people in society questioned it by mentioning that there is no justification for the general population to believe that these businesses will not continue to monetize this system and maintain this surveillance infrastructure once the pandemic is over, which is creating a contradicting view against volunteerism.

Accordingly, we believe that it is important to highlight that the concept of vulnerability in sharing personal information pertains to an individual's perception of the potential negative repercussions. This vulnerability escalates when individuals believe that disclosing personal information might result in threats, such as the abuse or misuse of that information.⁴⁵⁹ Although, during the COVID-19 pandemic, individuals may be willing to share their personal information for their own safety and the benefit of society, thereby when choosing between privacy and health, they might prioritize the latter,⁴⁶⁰ we believe there are still certain level of concerns due to the unique nature of the applications and its voluntary implementation.

We, thus, would like to reiterate the fact that the main purpose of contact tracing applications is to decrease the severity of the Covid-19 pandemic and the spread thereof while at the same time clearly protecting fundamental privacy rights, as detailed in Chapter 1. However, existence of other excuses would be subject to confusion in the eyes of data subjects. For instance, despite earlier assurances, Singapore confirmed that digital contact-tracing

⁴⁵⁷ Mauro, Aaron (2020) "Coronavirus contact tracing poses serious threats to our privacy." The Conversation, available at: <https://theconversation.com/coronavirus-contact-tracing-poses-serious-threats-to-our-privacy-137073> (accessed on 23 June 2024)

⁴⁵⁸ *Ibid.*

⁴⁵⁹ Sharma, Shavneet; Singh, Gurmeet; Sharma, Rashmini; Jones, Paul; Kraus, Sascha and Dwivedi, Yogesh K. (2020) "Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps", *IEEE Transactions on Engineering Management*, pp.1-17, p.8.

⁴⁶⁰ Tran, Cong Duc and Nguyen, Tin Trung (2021)"Health vs. privacy?...." op.cit., p.2.

data would be used for criminal investigation, which was beyond the initial purpose of data collection.⁴⁶¹ The latter was akin to the situation in Hong Kong in which digital contact-tracing data would primarily be used for tracking exposed individuals; they would and were also used for criminal investigation when needed in the absence of similar provisions in the COVIDSafe Act, which had massive impact on the user's trust against data controllers.⁴⁶² On the top of that, when such concerns related to excessive processing and abuse of data are combined with the mandatory use, it is not extremely difficult to perceive the potential concerns from the users' perspective.

Particularly, returning to the jurisdictional scope of our research, namely the EEA/EU, as introduced earlier that Portugal case for mandatory installation of the apps⁴⁶³ attracted huge reaction from scholars and, the Commission and the EDPB as there were serious concerns that this proposal of Portugal, since it involved mandatory installation and intrusive policing, constitutes a violation of fundamental rights to freedom and privacy, and also infringed national and European data protection laws.⁴⁶⁴ That was the first and the last proposal of mandatory use of the applications within the GDPR jurisdictions, which created a risk on the will of data subjects. Therefore, as mentioned, the download of the applications was on a voluntary basis by the EPDB⁴⁶⁵ and by the Chair of the Committee of Convention 108 and the Data Protection

⁴⁶¹ Kwan, Tsz Ho (2022) "Enforcement of the Use of Digital Contact-Tracing Apps in a Common Law Jurisdiction", *Healthcare*, MDPI, vol. 10, no. 9, p.1613 and 1619.

⁴⁶² Kwan, Tsz Ho. (2022) "Enforcement of the Use....", *op.cit.*, p.1619.

⁴⁶³ See Question for written answer E-005833/2020 to the Commission Rule 138 Lúcia Pereira (PPE), Paulo Rangel (PPE), José Manuel Fernandes (PPE), Álvaro Amaro (PPE), Maria da Graça Carvalho (PPE), Cláudia Monteiro de Aguiar (PPE Subject: Mandatory installation of contact tracing apps and personal data protection during pandemic https://www.europarl.europa.eu/doceo/document/E-9-2020-005833_EN.html (accessed 11 November 2022).

⁴⁶⁴ Parliamentary question - E-005833/2020, Mandatory installation of contact tracing apps and personal data protection during pandemic, https://www.europarl.europa.eu/doceo/document/E-9-2020-005833_EN.html (accessed on 30 March 2023).

⁴⁶⁵ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.6.

Commissioner of the Council of Europe.⁴⁶⁶ That being said, we believe that there are still other considerations we must consider for the voluntariness discussion in order to precisely delineate the all components of this risk type for any potential future use, even if they were not mandated by the controllers.

Suitably, as the second dimension of the voluntariness risk, we would like to highlight that, voluntariness is not all about perceived or subjective restrictions; someone who is deceived or manipulated may believe they acted freely when they did not.⁴⁶⁷ Similarly, an individual might feel their freedom to decide is restricted, even when, from an external perspective, it is not. This is particularly relevant in the context of individuals' decisions to contribute to public health, where a strong sense of civic responsibility could be perceived by the individual as a constraint on voluntary choice.⁴⁶⁸ Hence, there are, unfortunately, other barriers and risks existing in the way of implementing purely voluntary based processing. For example, there was also an implicit risk of being subject to mandatory contact tracing regime, such as using QR codes for entering indoor areas or to travel, which is as dangerous as explicit obligatory acts, and completely contradicting with fundamental principles of the European Law. Accordingly, for many scholars, mandate of digital contact-tracing app and vaccination in certain premises would restrict the freedom of movement and right to privacy,⁴⁶⁹ which we strongly agree with. In more detail, these scenarios can be seen as existing on a spectrum of public to private interference with individual liberty, ranging from public transport regulations to social norms at home.⁴⁷⁰ Setting aside the issue of actual legal permissibility

⁴⁶⁶ Alessandra Pierucci, Jean-Philippe Walter (2020) "*Joint Statement on Digital Contact Tracing...*", *op.cit.*, p.4.

⁴⁶⁷ Kamphorst, Bart A., Marcel F. Verweij, and Josephine AW van Zeben. (2023) "On the voluntariness of public health apps: a European case study on digital contact tracing." *Law, Innovation and Technology* 15, no. 1, pp.107-123, p.112.

⁴⁶⁸ Kamphorst, Bart A., Marcel F. Verweij, and Josephine AW van Zeben. (2023) "On the voluntariness of public health apps...", *op.cit.*, p.112.d.

⁴⁶⁹ Kwan, Tsz Ho. (2022) "Enforcement of the Use....", *op.cit.*, p.1619.

⁴⁷⁰ Kamphorst, Bart A., Marcel F. Verweij, and Josephine AW van Zeben. (2023) "On the voluntariness of public health apps...", *op.cit.*, p.114.

in different Member States, each scenario illustrates a distinct context in which the use of a contact tracing app may effectively be required, even if the app is officially offered by the State to the public on a voluntary basis,⁴⁷¹ which we believe also a risk to the individual's freedom to choose these applications voluntarily.

Moreover, as another component of on the term of voluntariness, there is a dimension on the real chance of selection after voluntarily downloading the application. For instance, once the app is downloaded, its usage may be mandatory, opt-in, or opt-out.⁴⁷² Nonetheless, even if downloading the app is optional, location sharing might be nonvoluntary and continuous, which we find quite detrimental for the voluntariness as well.⁴⁷³ Therefore, it might be deceiving the users in the end. However, there are also other impediments linked to implementing specific consent procedures such as language barriers, lack of customizable contact tracing apps, lack of comprehension, and absence of choice to deny consent.⁴⁷⁴ It is an important part of volunteerism with regards to the use of the applications, and viable risk, since it creates difficulties in revoking the consent, or providing opt-in for certain features of the applications. In this regard, interestingly, as proposed by Chen and Najam, once a pandemic is at stake, protecting one's (and the public's) health should be primary, but based on the behavioral immune system, they found that greater social conservatism and valuation of personal privacy may be greater than both personal and public health concerns.⁴⁷⁵ Such a quantitative approach could also solidify our perspective that users' feelings

⁴⁷¹ Kamphorst, Bart A., Marcel F. Verweij, and Josephine AW van Zeben. (2023) "On the voluntariness of public health apps...", op.cit., p.114.

⁴⁷² Hogan, Katie; Macedo, Briana; Macha, Venkata; Barman, Arko and Jiang, Xiaoqian (2021) "Contact tracing apps: lessons learned on privacy, autonomy, and the need for detailed and thoughtful implementation", *JMIR Medical Informatics*, vol. 9, no. 7, e27449, pp.1-20, p.7.

⁴⁷³ *Ibid.*

⁴⁷⁴ Mbunge, Elliot (2020) "Integrating emerging technologies ..." op.cit., p.1634.

⁴⁷⁵ Chan, Eugene Y., and Saqib, Najam U. (2021) "Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high." *Computers in Human Behavior*, vol.119, 106718, pp. 1-13, p.1.

of implicit obligation could be even more scary for them. Although we are not entirely convinced about such distinct approach over the health and privacy dilemma, we definitely understand that it is also about the value that users attributes to their privacy protection. Therefore, such approach increases the risks around the voluntary use as well as obliged features of the applications. However, given that many of the European applications are not massively reliant on a consent mechanism for the processing as well as different features of the application, this risk has a less material impact on data subjects, whose potential solutions are to be addressed in Chapter 3 under consent requirement.

As such, in any case, if the EEA data subjects would feel pressured, thereby obliged about the use of these applications, as the global counterparts highlighted in Chapter 1, it would be hazardous for the proper implementation of the right to privacy set out in the EU Charter of Fundamental Rights.⁴⁷⁶ In particular considering the lawful basis of the data controllers detailed in Chapter 3, vast majority of them were relying on “safeguarding public health” as per the Article 9-2-I of the GDPR ⁴⁷⁷ as a lawful basis, room for consent mechanism for processing features is limited by the regulators. Hence, it is plausible to conclude that risks related to the obligation to use of contact tracing applications are the least severe risk among others delineated in this Chapter, due to the nature and application of laws. Nevertheless, it is still important to take necessary steps so that a lawful basis other than consent will not end up in damaging scenarios, which will be addressed in Chapters 3.

7. Transparency and Accountability Risks

Another drastic risks that attract the attention of users are the issue of transparency and accountability of data controllers. In case there is not fully

⁴⁷⁶ Article 8 of the EU Charter of Fundamental Rights.

⁴⁷⁷ Article 9-2-I sets out that processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

transparent and accountable approach of controllers, many data subjects would not know whom the data controls, the data protection officer, and, if any, the data processor of the contact tracing applications used in that country/this situation causes serious problems in terms of accountability of controllers. In other words, data subjects would not know whom they would hold responsible against them in case they have an aspiration to use their rights without a possible violation, and to whom they would direct these rights before the third parties. Therefore, transparency and accountability risks related to contact tracing activities goes together due to their closely interconnected nature.

Correspondingly, the term accountability has many aspects, and once calling out the term of accountability, it is important to note that privacy policies pose a challenging requirements problem for organizations due to comprehensiveness, which includes describing data practices across physical places where business is conducted (e.g., stores, offices, etc.), as well as web and mobile platforms; and accuracy, which means all policy statements must be true for all data practices and systems.⁴⁷⁸ Accordingly, the issue of who would be held responsible for data processing, and activities in contact tracing applications is an issue that involves several components and creates lots of privacy risks due to the vagueness of these terms. The fundamental reason of this situation is that the applications in question are offered not only by the state, i.e. data controllers, but also by the third-party actors, i.e. data processors, as introduced above. As such, according to the principle of "accountability" stipulated by the GDPR, whoever owns the application in question appears to be accountable by the GDPR⁴⁷⁹. To be more definitive, since the GDPR covers, including but not limited to, the processing activities of legal entities⁴⁸⁰, the application carried out by both methods will also fall

⁴⁷⁸ Bhatia, Jaspreet, Travis D. Breaux, Joel R. Reidenberg, and Thomas B. Norton (2016) "A theory of vagueness and privacy risk perception", *2016 IEEE 24th International Requirements Engineering Conference (RE)*, pp. 26-35, p.26.

⁴⁷⁹ Article 5-2 of the GDPR: accountability.

⁴⁸⁰ Article 3-1 of the GDPR: material scope.

within the subject of the GDPR. Within the same remit, the relationship between the data controller, data processor, and data protection officer, with GDPR origin, causes risks by creating ambiguity among the responsibilities and accountabilities of each of them.

Consequently, data subjects would feel threatened for their right to privacy and data protection, in case they are not provided a clear explanation of the separation of tasks and protection levels provided by data controllers and data processors, and its reflection on contact tracing applications would be in the form of distrust against the data controller, namely ministry of health of the countries. It would, hence, automatically raise skepticism among data subjects regarding breaches concerning the fundamental privacy rights of whole European citizens stipulated under article 8 of the Charter of Fundamental Rights.⁴⁸¹, which situation may pose more difficulties in applying these sanctions to the applications owned by the state, as these applications are not managed only by private companies. In more detail, the power of state institutions to observe whether citizens are infected is more centralized within the scope of providing a more centralized observation and access to data from a single center. However, the identity and number of state authorities implementing such pandemic monitoring activities is of huge importance. In case there is not clear distinction between the roles and responsibilities, or access rights of certain authorities to processed data subject to central review, data controllers could feel vulnerable to excessive processing activities. Therefore, the interplay between accountability and transparency could lead to drastic privacy concerns in the eyes of the data subjects, due ambiguity of roles and surveillance activities of different public actors, which was particularly raised by the AEPD decisions on Radar Covid application detailed in Chapter 7.

Suitably, this is particularly relevant for identifiable data, but it also remains relevant for all data provided on the premise (and with the consent) that they

⁴⁸¹ Article 8 of the Charter of Fundamental Rights: protection of personal data.

are to be used specifically for contact tracing or public health surveillance.⁴⁸² Where there is a possibility that data may be used to improve the management of future public health crises, this should be stated in advance; at a minimum, data can be de-identified, and a clear and public announcement made to provide justification for their use at a later date.⁴⁸³ The necessity of explaining in detail to data subjects creates certain privacy risks for data controllers to remediate. Accordingly, as concluded by the study of Michel Walrave, Cato Waeterloos, and Koen Ponnet, a perceived barrier for some potential users is privacy concerns.⁴⁸⁴ Therefore, when creating and launching an application, an explanation of how individuals' privacy is protected is required,⁴⁸⁵ failure to which would again exacerbate lower acceptance levels of the applications. This perspective is also supported by our proposal elaborated on in Chapter 4. The underlying reason for such an approach is that users would potentially be affected by privacy-related disaster scenarios as well. Such scenarios are widely mentioned in different channels of communication, and naturally, users might be deterred by the potential adverse effects of digital contact tracing applications. Within the same vein, a supporting idea for this situation could be derived from the study of Huckvale and colleagues. They provided in their research that in case patients or the public are deterred from using applications, potential clinical benefits of mobile health are not realized due to trust issues.⁴⁸⁶ Although the scope of the research is related to unaddressed data protection risks in accredited health and wellness applications, rather than contact tracing applications, it is notable to witness a similar perspective with regard to the

⁴⁸² Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing ...", *op.cit.*, p.23.

⁴⁸³ Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing ...", *op.cit.*, p.24.

⁴⁸⁴ Walrave, Michel; Waeterloos, Cato and Ponnet, Koen (2020) "Adoption of a Contact Tracing App....", *op.cit.*, p.7.

⁴⁸⁵ *Ibid.*

⁴⁸⁶ Huckvale, Kit; Prieto, José Tomás; Tilney, Myra; Benghozi, Pierre-Jean and Car, Josip (2015) "Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment", *BMC medicine*, vol. 13, n.1, pp. 1-13, p.12.

use of applications, namely due to trust-related reasons. The type of personal data might be similar in the sense that personal data subject to processing activities within the scope of health and wellness applications are categorized as also a special category of personal data under Article 9 of the GDPR.⁴⁸⁷ We, hence, are of view that the same risk type is also applicable to contact tracing applications, and can generate a potential red flag at the outset of the processing activities.

Furthermore, in a similar context, the research of Kolasa and colleagues emphasized the privacy risk generated by this, and provided the critical success factors in this realm revolve around transparency and targeted information campaigns aimed at individuals, achieved through raising awareness of citizen responsibility and offering pertinent details on data protection and cybersecurity.⁴⁸⁸ Fostering citizen engagement in public affairs, like public health, contributes to individuals feeling a sense of belonging to the state.⁴⁸⁹ This heightened awareness would encourage individuals to willingly share their data within a secure and regulated environment, ultimately benefiting society as a whole.⁴⁹⁰ Otherwise, such lack of awareness, would contradict the general approach regarding the interplay between the transparency acts of controllers and its consequences on diminishing the concerns related to data protection-related matters, as elaborated in the following sections, and briefly mentioned in the previous chapter complying with the transparency requirement under the GDPR.⁴⁹¹ That being said, obviously, not only notifying people regarding the type of

⁴⁸⁷ See Article 9 of the GDPR, processing of special categories of personal data.

⁴⁸⁸ Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review", *JMIR mHealth and uHealth*, vol.9, n.6, e23250, pp.1-11, p.7.

⁴⁸⁹ Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the Art in Adoption of Contact Tracing Apps...", *op.cit.*, p.7.

⁴⁹⁰ *Ibid.*

⁴⁹¹ See Article 13 and 14 of the GDPR, Information to be provided where personal data are collected from the data subject and Information to be provided where personal data have not been obtained from the data subject, respectively.

processing activities would be deemed sufficient to mitigate these risks and concerns, whose nuances is elaborated in Chapter 3 for the EEA/EU applications and Chapter 7 for the Spanish application.

Correspondingly, in this regard, the research implemented by Youn defended the idea that concerns for privacy are heightened when consumers feel uninformed about who is collecting their personal information, how companies obtain their information, or for what purposes the information is used.⁴⁹² Such negative feelings may motivate consumers to avert risks associated with divulging personal information to marketers.⁴⁹³ Even though this study deals with online privacy concerns, we are of the view that there is still a context that might be extracted for the digital contact tracing-related risks as well. To be more specific, for contact tracing activities, we can also support the idea that in line with the aforementioned concerns, such negative feelings related to the interplay between digital contact tracing activities and data processing activities, users feel less willing to provide their personal data to data controllers, thereby giving up on the use of contact tracing applications. In other words, the potential interest of a third-party developer company that is also engaging in marketing activities may not genuinely consider the best interest of data subject users, as their primary goal is to generate a monetary benefit from the personal data processed. While the primary strategy collects information about covid symptoms, the positive test, and contacts in a central database that is subsequently available for epidemiological and public health purposes, which, again, would end up in a situation that users feel discouraged to provide their personal data to data controllers.

Moreover, as another source of concern within the transparency and accountability remit is the risk of third party involvements to the process, as briefly introduced in Chapter 1. In other words, although fear of surveillance

⁴⁹² Youn, Seounmi (2009) "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents", *Journal of Consumer affairs*, vol. 43, no. 3, pp. 389-418, p.392.

⁴⁹³ Youn, Seounmi (2009) "Determinants of online privacy concern...", op. cit., p.392.

from the government was expressed in numerous studies, privacy matters not only about the authorities.⁴⁹⁴ Accordingly, the identity of the app developers seems to matter, as well as privacy in relation to other individuals.⁴⁹⁵ The ministry of health or any public authority appointed in this regard could attain the location data of the citizens that they can follow with the GPS method, together with their names via their mobile phones, as will be detailed in the following chapter. While walking on a street, it can be annoying for many people that even their neighbors go to the window and follow where they go and at what times they do them. As such, knowing that these data are also obtained by data controllers and third parties, who are likely to share this data can also create stress and insecurity for citizens in society.

That being said, the study of Hassandoust and colleagues found that as an individual's feeling that their right to privacy would be protected increases, so too does their trust in the public health authorities' ability to handle their sensitive personal data.⁴⁹⁶ This certainly contributes to the explanation of why the most significant determinant of data privacy concerns was information sensitivity.⁴⁹⁷ However, it is also crucial to remember that, as Oomen and Ronald pointed out, how each person perceives these hazards depends on their own values, general perceptions, and experiences.⁴⁹⁸ We concur with their opinion, considering that the type of feared events in terms of privacy breaches that each data subject ever witnessed or actually experienced could definitely be a multiplying factor for their risk perception. As stated by Evans

⁴⁹⁴ Oyibo, Kiemute; Sahu, Kirti Sundar; Oetomo, Arlene and Morita, Plinio P. (2021) "Factors influencing the adoption of contact tracing applications: Protocol for a systematic review", *JMIR Research Protocols*, vol. 10, no. 6, e28961, pp.1-20, p.16.

⁴⁹⁵ *Ibid.*

⁴⁹⁶ Hassandoust, Farkhondeh; Akhlaghpour, Saeed and Johnston, Allen C. (2021) "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective", *Journal of the American Medical Informatics Association*, vol.28, no. 3, pp. 463-471, p.469.

⁴⁹⁷ Hassandoust, Farkhondeh; Akhlaghpour, Saeed and Johnston, Allen C. (2021) "Individuals' privacy...", op.cit. p.469.

⁴⁹⁸ Oomen, Isabelle, and Leenes, Ronald (2008) "Privacy risk perceptions and privacy protection strategies", *Policies and research in identity management*, pp. 121-138. Springer, Boston, p.122.

and colleagues, good risk communication depends on understanding more than quantitative risks and benefits; background experiences and values also influence the process.⁴⁹⁹ Hence, the value of privacy risk is something more than quantitative and could end up in undesired situations for data subjects about their private life. For sure, we do not support the idea that privacy prevails over the right to live, yet as mentioned during each part of the thesis, we are of the perspective that striking a balance between these two rights is strictly associated with the success of contact tracing applications.

Additionally, identical to these worries, a potential contact tracing mobile applications adopter's fear for their privacy grows as the sensitivity of the data submitted to contact tracing mobile applications rises. Additionally, the extent to which individuals sense discomfort and privacy issues is influenced by the sort of information that is gathered and used by third parties, according to a large body of studies.⁵⁰⁰ We, thus, believe that this study shed light on the importance of the privacy perception of the users. However, at the same time, risks related to the collection, utilization, and storage of private information by a digital tool, as well as worries about contact tracing apps being repurposed to introduce and normalize increased, automated, and routine population surveillance for goals other than preventing the transmission of infectious diseases are among the issues that need to be addressed.⁵⁰¹ As such, some academics pushed for a "decentralized" method of digital contact tracking based on solution offered by Google and Apple, in which devices often share random numbers that stay on users' phones. It is important to note that researchers must also pinpoint the underlying causes of privacy difficulties in

⁴⁹⁹ Evans, Geoffrey; Bostrom, Ann;. Johnston, Richard B.; Fisher, Barbara Loe and Stoto, Michael A. (1997) "Risk communication and vaccination: summary of a workshop.", Institute of Medicine (US) Vaccine Safety Forum. Risk Communication and Vaccination: Summary of a Workshop. Washington (DC): National Academies Press (US); 1997. PMID: 25121223, p.4.

⁵⁰⁰ Hassandoust, Farkhondeh; Akhlaghpour, Saeed and Johnston, Allen C. (2021) "Individuals' privacy...", op.cit. p.469.

⁵⁰¹ Samuel, Gabby; Roberts, Stephen L.; Fiske, Amelia; Lucivero Federica; McLennan, Stuart; Phillips, Amicia; Hayes, Sarah and Johnson, Suzanne B. (2022) "COVID-19 contact tracing apps: UK public perceptions", *Critical Public Health*, vol.32, n.1, pp. 31-43, DOI: 10.1080/09581596.2021.1909707, p.33.

order to investigate privacy issues thoroughly.⁵⁰² Nearly all evidence-based privacy research in social scientists relies on the quantification of a privacy-related proxy of some kind due to the difficulty and inconsistent nature of defining and measuring privacy holistically, also the fact that the notable relationships rely more on cognitions and perceptions than on reasoned assessments.⁵⁰³

Suitably, on the perceptual aspects, Bhatia and colleagues define privacy risk perception as the act of identifying a choice or action that may have an impact on privacy.⁵⁰⁴ Therefore, we believe it is reasonable to state that the threat posed by data processing activities of contact tracing applications could strongly depend on the personal identification of data subject users. As such, choice and identification do not have to be rational each time. For instance, while some users are intimidated by location tracking that could take place within the scope of digital contact tracing, others can be more anxious about the processing of their health data and its storage. Moreover, in relation to the correlation between the level of awareness and privacy concerns, the study of Udoh and colleagues could provide helpful insight, even though the source of data protection concerns is different activities. Accordingly, as per their study, the data protection concerns stated do not appear to be associated with the level of awareness of the smartwatch privacy risks.⁵⁰⁵ As a matter of fact, while some participants who were aware of the risks said they did not care about potential data protection violations, there were also others who are unaware, yet very concerned about possible data protection violations.⁵⁰⁶

⁵⁰² Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy...", *op.cit.*, p.800.

⁵⁰³ Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy...", *op.cit.*, p.800.

⁵⁰⁴ Bhatia, Jaspreet; Breaux, Travis D.; Friedberg, Liora; Hibshi, Hanan and Smullen, Daniel (2016) "Privacy risk in cybersecurity data sharing", *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 57-64, p.58.

⁵⁰⁵ Udoh, Emmanuel Sebastian, and Alkharashi, Abdulwahab (2016) "Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students", *Future Technologies Conference (FTC)*, pp. 926-931, p.929.

⁵⁰⁶ Udoh, Emmanuel Sebastian, and Alkharashi, Abdulwahab (2016) "Privacy risk awareness...", *op.cit.*, p.929.

From our perspective, nevertheless, there is another aspect of the awareness issue. To be more concrete, for example, the level of awareness could have a detrimental effect on the risk appetite of the people. In case people are not receptive to facing any new privacy risk at the cost of preventing the spread of the virus, their risk appetite might potentially be conversely affected. In other words, the more people learn about the potentially detrimental outcomes of privacy breaches, the less they are willing to download such applications. For instance, per the study by Gasteiger and colleagues, in which they implemented qualitative and quantitative data were gathered from a nationwide online survey to explore the barriers and facilitators to the New Zealand general public's use of the COVID-19 contact tracer app, a minority of participants reported data protection and security concerns, which deterred them from the using the app.⁵⁰⁷

To provide further detail thereon, certain participants mentioned learning about these privacy concerns from their family members and the broader public.⁵⁰⁸ Similarly, Zhang's study on data protection and surveillance perception found evidence that the public holds misinformed beliefs about contact tracing apps even after reading about how the apps work. Nevertheless, these misinformed beliefs were not associated with opposition to downloading and using the apps.⁵⁰⁹ Hence, as seen, the risk is not only related to people's awareness, but also to the wrong awareness sometimes. In line with this concern, there is another significant idea provided by study of Bellekens and colleagues. Their study indicated that risk awareness in the context of cyber-security is crucial to how people act and make decisions

⁵⁰⁷ Gasteiger, N., Gasteiger, C., Vedhara, K., & Broadbent, E. (2022). The more the merrier! Barriers and facilitators to the general public's use of a COVID-19 contact tracing app in New Zealand. *Informatics for Health and Social Care*, 47(2), 132-143, p.142.

⁵⁰⁸ *Ibid.*

⁵⁰⁹ Zhang, Baobao, Sarah Kreps, Nina McMurry, and R. Miles McCain. (2020)"Americans' perceptions of privacy and surveillance in the COVID-19 pandemic." *Plos one* 15, no. 12, p. e0242652.

when confronted with a cyber threat.⁵¹⁰ It might be challenging to persuade users to abide by established regulations because it depends on their knowledge and comprehension.⁵¹¹ Overall, as discussed widely across the literature on privacy risk, which we also agree with, there is not only the transparent communications, but also accuracy, perceivability and comprehensiveness of such information matters. Failure to comply with this subset of transparency would then end up in risk on data subjects as well.

Within the similar vein, considerable number of studies have also found a strong link between privacy worries and privacy-management practices.⁵¹² For example, within the domain of e-commerce, concerns in relation to online privacy matters are linked with engaging in privacy-protective behaviors such as removing one's personal information from commercial databases, deleting cookies, and refraining from self-disclosure.⁵¹³ We agree with this findings, as people tend to be more diligent about any potential disclosure of commercial activities. Accordingly, we also believe that such privacy concerns of users play an important role in their data management decisions, but it does not necessarily mean that they would completely be against downloading contact tracing applications. Thus, the risk related to transparent information does not always mitigate by further explanations by controllers, as the risk perception of the users also differs massively.

In line with this logic, as shown by the research of Van Zoonen, there is a simultaneous absence of acceptable secure behavior despite people's clearly articulated concerns regarding their privacy, the most common pin code is

⁵¹⁰ Bellekens, Xavier; Hamilton, Andrew; Seeam, Preetila; Nieradzinska, Kamila; Franssen, Quentin and Seeam, Amar (2016) "Pervasive eHealth services a security and privacy risk awareness survey", international *Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pp.1-4, p.1.

⁵¹¹ *Ibid.*

⁵¹² Baruh, Lemi; Secinti, Ekin and Cemalcilar, Zeynep (2017) "Online privacy concerns and privacy management: A meta-analytical review." *Journal of Communication*, vol. 67, no. 1, pp. 26-53, p.27.

⁵¹³ Baruh, Lemi; Secinti, Ekin and Cemalcilar, Zeynep (2017) "Online privacy concerns and privacy management...", op.cit., p.27.

1234, and many people use the same password for numerous accounts.⁵¹⁴ Nevertheless, at the same time, people provide their personal details on various social media platforms even if they do not feel particularly secure on sites like Facebook, for example.⁵¹⁵ This discrepancy between concerns and conduct is referred to as the "privacy dilemma" in the pertinent literature. As a result, people may make irrational decisions that cause them to reject new security measures because they believe they would not be beneficial.⁵¹⁶ Unlike previously identified data watchers, these data watchers do not have the best interests of their data sharers in mind.⁵¹⁷

Also, differently, it is important to introduce the term the privacy paradox, which corresponds to a phenomenon where people express concerns about revealing personal information yet act in a way that contradicts those concerns, which may assist in explaining this.⁵¹⁸ In other words, even though users fear disclosing their personal information to other parties to use this application they are still doing this to use the application. This notion was also analyzed by the study by Baruh and colleagues, who noted that many studies have found that people's data protection concerns do not always correspond with the privacy management decisions they make, a phenomenon known as the "privacy paradox"⁵¹⁹, which we believe could be interesting and leveraged for contact tracing approach as well, resulting in the potential situation that no matter how data controllers provided privacy notice to the users, there could

⁵¹⁴ Van Zoonen, Liesbet (2016) "Privacy concerns in smart cities", *Government Information Quarterly*, vol. 33, no. 3, pp. 472-480, p.474.

⁵¹⁵ Van Zoonen, Liesbet (2016) "Privacy concerns...", *op.cit.*, p.474.

⁵¹⁶ Hong, Jason I.; Jennifer D. Ng; Lederer, Scott and Landay, James A. (2004) "Privacy risk models for designing privacy-sensitive ubiquitous computing systems", *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pp. 91-100, p.95

⁵¹⁷ Hong, Jason I.; Jennifer D. Ng; Lederer, Scott and Landay, James A. (2004) "Privacy risk models for designing privacy-sensitive...", *op.cit.*, p.95.

⁵¹⁸ Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the Art in Adoption of Contact Tracing Apps...", *op.cit.*, p.7.

⁵¹⁹ Baruh, Lemi; Secinti, Ekin and Cemalcilar, Zeynep (2017) "Online privacy concerns and privacy management...", *op.cit.*, p.27.

be still some concerns in their eyes, or conversely, even more aspiration to use the apps due to such paradox, even if controller clearly indicates all the privacy risks associated with contact tracing activities. Though these cases would not be extremely common, but we would still want to highlight it by collating different views in the literature and presenting our idea to indicate intricacies of concerns thereon.

Hence, considering the aforementioned discussions on the actual risks and perceived risks of data subjects, it is plausible to conclude that there are many risk drivers and sources of concerns with regard to the transparency and accountability of data controllers due to several reasons. In addition, we believe that the type of risks and concerns could be even varied and reach to countless level by considering sub-components described above. Nevertheless, the most important thing is to focus on key risks and develop potential safeguards to mitigate these risks. The main safeguards and recommendations to mitigate such risks are scrutinized in Chapter 3, 4 and 5, as per the GDPR and the other key regulations and guidance in EEA/EU. From our perspective, a key takeaway from these listed and detailed concerns is to understand the deficiencies of contact tracing applications in the eyes of data subject users. As explained above, their positive attitude regarding the use of contact tracing applications is key to achieving widespread use of contact tracing applications, thereby combating any pandemic.

**PART TWO- EUROPEAN REGULATORY
FRAMEWORK FOR CONTACT TRACING
APPLICATIONS**

III- LEGAL BASIS, GENERAL GDPR PRINCIPLES AND DATA SUBJECT RIGHTS UNDER THE GDPR

1. **GDPR Principles and Contact Tracing Applications**

Regarding the legal regime contact tracing applications are subject, the GDPR is undertaking a significant role in the EEA⁵²⁰. The GDPR was designed and approved by the EU, and it imposes requirements on enterprises anywhere that target or collects data about EEA citizens.⁵²¹ Therefore, it is plausible to state that the GDPR legislation's purpose is to provide data subjects complete control over their personal data by defining several rights,⁵²² including but not limited to the rights of contact tracing app users. Similarly, the ePrivacy directive⁵²³ also applies to contact tracing-related matters to the extent that digital contact tracing activities fall within the scope of processing personal data in the electronic communications sector.

Establishing an entirely new legal regime for contact tracing applications would be extremely lengthy and complex, since there are already inherent risks linked to contact tracing applications, as detailed in Chapter 2, and the need for the applications were urgent. Therefore, the most realistic option was to compress the data protection and privacy aspects of the contact tracing applications used in relation to the pandemic, into the current privacy system i.e., the GDPR and ePrivacy Directive, which are mentioned by the

⁵²⁰ EEA Agreement, Annex XI, Protocol 37, amended by Decision of the EEA Joint Committee No 154/2018, of 6 July 2018.

⁵²¹ Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) available at <https://gdpr.eu/what-is-gdpr/>, (accessed on 03 August 2023).

⁵²² *Ibid.*, Chapter III, Rights of the data subject, arts. 12-23.

⁵²³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (the "ePrivacy Directive).

Commission regarding contact tracing applications as well⁵²⁴, to provide further context based on the interpretation thereof. Accordingly, the EDPB requires all data controllers to act on a complaint basis to themselves.⁵²⁵ Reflecting the unity sought by the European Union in a legal context, there's an emphasis on aligning laws and directives. The Commission's approach to contact tracing applications highlights this by referencing both the directives and the GDPR. It outlines specific features and standards that these apps should adhere to, aiming for compliance with EU regulations concerning privacy and the protection of personal data.⁵²⁶ To this end, the EPDB published a guideline on the contact tracing subject on April 20, 2020,⁵²⁷ as briefly touch based in Chapter 1. Even though this guideline and the Commission's guidelines⁵²⁸ are jointly providing context to the contact tracing applications from the European perspective on the contact tracing matters, they should not be interpreted as a stand-alone source, as both of which contain serious references to the GDPR.

Therefore, in Chapter 3 and 4, we will assess the compliance efforts of contact tracing applications from legal and technological point of view under the GDPR requirements, and provide tailor-made recommendations for further

⁵²⁴ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024) section 1 para. 5.

⁵²⁵ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

⁵²⁶ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024), section 1 para. 5.

⁵²⁷ EDPB (2020) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed on 23 June 2024) These Guidelines were adopted following art. 70(1)(e) GDPR procedure.

⁵²⁸ eHealth Network (2020), Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, available at https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf (accessed on 23 June 2024).

development areas to achieve most privacy friendly version thereof by considering the potential future needs in the same remit as well, given that compliance with these principles set out under the GDPR are also measuring the sufficiency of how they have responded to the risks delineated in Chapter 2.

2. Concrete recommendations on Legal Basis of Processing, Data Minimization, Purpose Limitation, Consent and Transparency Requirements, and Data Subject Rights

2.1 Legal Basis of Contact Tracing Applications

Data controllers, both public and private entities, continue to be subject to standard data protection rules even in emergency circumstances⁵²⁹, due to the aforementioned reasons. Accordingly, their obligation to rely on a legal basis remains essential to guarantee the lawfulness of processing operations.⁵³⁰ The lawfulness for processing activity was set out under Article 6 of the GDPR⁵³¹. Furthermore, Art. 9(1) “ePrivacy” Directive⁵³² also sets out the consent mechanism as for the legal basis of processing activities. Among

⁵²⁹ Ventrella, Emanuele (2020) “Privacy in emergency circumstances: data protection and the COVID-19 pandemic”, ERA Forum, n.21, <https://doi.org/10.1007/s12027-020-00629-3>, pp.379–393, p.381.

⁵³⁰ Ventrella, Emanuele (2020) “Privacy in emergency circumstances....”, *op.cit.*, p.381.

⁵³¹ Article 6 of the GDPR, Lawfulness of Processing states the legal basis of processing.

⁵³² Article 9(1) of the “ePrivacy” Directive sets out “where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value-added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.”

the legal basis, consent under the 9(2)(i) GDPR⁵³³, and Art. 9(1) “ePrivacy Directive, public interest or art. 9(2)(i) GDPR, namely health care purposes are relied upon by data controllers of contact tracing applications our research on their privacy policies that is detailed in Chapter 1.

Although consent might seem like the safest approach under GDPR and 'ePrivacy' regulations, the urgency of public health measures allows for processing not solely dependent on consent but also on other legal bases stipulated in Article 6(1)(e) of the GDPR. Hence, public interest plays important role in processing activities of the applications. We are, thus, of a view that is also indicated by the EDPB like a reference to the voluntary nature of the application and specification of purpose and explicit limitations of further processing, regardless of the legal basis, it is important to keep acting in line with the spirit of the GDPR and ePrivacy Directive for the lawful basis of processing activities within the contact tracing activities. Furthermore, the processing activity should not be disproportionate, and it should indicate true needs and medical relevance, should be limited for the duration of the Covid-19 crisis.

Accordingly, in line with the discussions pertaining to legal grounds set out under the GDPR, the EDPB also indicated its direction by setting forth that The requirement for the performance of a task in the public interest, i.e., Art. 6(1)(e) GDPR, appears to be the most pertinent legal basis for the processing when public authorities provide a service based on a mandate assigned by and in accordance with requirements laid out by law.⁵³⁴ Relevant personal data other than special category data can be processed for the purposes

⁵³³ Pursuant to Article 9(2)(i) of the GDPR “processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy”.

⁵³⁴ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.9.

outlined above in accordance with both Art. 6(1)(d)⁵³⁵ and (e)⁵³⁶ of the GDPR. While the initial legal basis allows processing personal data that is necessary to protect the vital interest of individuals (i.e., to save lives), the second can be relied upon to protect the public interest or in the implementation of official authority granted to data controller. Given that the determination of public interest is exclusively within the jurisdiction of Union or Member State law, Recital 46 of the GDPR explicitly identifies epidemic monitoring as a context in which processing can serve both critical public interest objectives and the vital interests of data subjects.⁵³⁷ Concerning health data, a legal basis for processing can be found in Art. 9(2)(i) GDPR, and further guidance is provided by Recitals 52 and 54 GDPR.⁵³⁸ As per the Article 5-3 of the ePrivacy Directive, the storage of information can only be retained on a user's device or accessed if the user has provided permission or if the storage and/or access are strictly required for the information society service that the user has specifically requested.⁵³⁹ Therefore, we are of the perspective that rather than merely focusing on the consent as a lawful basis, it is more practical to utilize other legal grounds for processing activities while at the same time implementing certain safeguards alongside, as detailed in the following sections. However, we also believe that this does not necessarily mean that

⁵³⁵ Article 6(1)(d) of the GDPR sets out that “processing is necessary in order to protect the vital interests of the data subject or of another natural person”.

⁵³⁶ Article 6(1)(e) of the GDPR sets out that “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.

⁵³⁷ Ventrella, Emanuele (2020) “Privacy in emergency circumstances....”, *op.cit.*, p.381.

⁵³⁸ Ventrella, Emanuele (2020) “Privacy in emergency circumstances....”, *op.cit.*, p.381.

⁵³⁹ Article 5-3 of the ePrivacy Directive sets out that “Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.” Available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>.

consent is not an efficient mechanism. Particularly, we recommend more room for consent, if not for the main lawful basis, at least for the different type of processing activities or activation of other features on more active basis than it is.

In line with this approach, the EDPB also listed the circumstances where data controllers may rely on different legal grounds, rather than consent, i.e., vital interest of the individual and preserving public health.⁵⁴⁰ This one is, surely beneficial for data controllers for their determination of lawful basis. Nonetheless, from our perspective, the indication of such legal grounds for processing activities must be tailor-made for each contact tracing application. The fundamental reason behind our perspective is that while the GDPR sets out the general rules pertaining to privacy, it is data controllers' duty to solidify such rules with their efficient implementation based on their interpretation. For instance, as a prerequisite of consent legal basis, transparency requirements demand that companies not only ensure all the required information does contain, but also that such information is provided in a readable, comprehensible format.⁵⁴¹ Ultimately, organizations should keep in mind that the GDPR's fundamental objective is to give each data subject the information they require about any processing of their personal data and what their rights are connected to that processing so they can decide if they desire to exercise those rights.⁵⁴²

Nonetheless, we believe that although these requirements establish the fundamental expectation from data controllers of any processing activities, including digital contact tracing, the manner of the notice requirement must be adopted by data controllers of the contact tracing applications as in line with the current technology and potential vulnerabilities of contact tracing

⁵⁴⁰ EDPB (2020) Guidelines 04/2020, *op. cit.*, p.9.

⁵⁴¹ Matheson, Lee (2018) "Top 10 Operational Responses to the GDPR – Part 6: Transparency and privacy notices", IAPP, [https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-6-transparency-and-privacy-notice/#:~:text=Pursuant%20to%20Article%2012\(1,the%20disclosure%20should%20be%20easily](https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-6-transparency-and-privacy-notice/#:~:text=Pursuant%20to%20Article%2012(1,the%20disclosure%20should%20be%20easily) (accessed on 15 June 2024).

⁵⁴² *Ibid.*

applications. Therefore, in this regard, we think that data controllers must review their notices and legal grounds on a regular basis. Sending SMS and e-mails to the users about the updates on privacy policies seems a more straightforward solution than posting a notice on the contact tracing applications, as also detailed in the next Chapter under Notice section. The reason is users are assumed to spend more time with their phones and emails than logging in to their contact tracing applications. By this method, efficient implementation of any legal basis could be achieved by data controllers of contact tracing applications, by complying with the notice requirements of the GDPR⁵⁴³. Similarly, with regards to the lawful basis in the real-life implementation, as for the case of the Lithuanian application called 'Karantinas', which was designated as a symptom tracking application, Lithuanian Data Protection authority imposed fine both on the National Public Health Centre (NPHC) and the developer of the application UAB "IT sprendimai sėkmei" (the Company).⁵⁴⁴

Lithuanian Data Protection Authority rendered that given that the NPHC and the Company failed to justify the legality of the processing of activity performed by the application, the DPA determined that the app had failed to uphold the requirement of Article 5(1) of the GDPR.⁵⁴⁵ As neither the NPHC nor the Company acknowledged that they were data controllers at the time of the inspection, both denied their liability as data controllers and accordingly failed to implement the principle of accountability enshrined in Article 5(2) of the GDPR and the principle of transparency was also violated by providing incorrect information about data controllers and processors in the

⁵⁴³ See Article 13 of the GDPR, Information to be provided where personal data are collected from the data subject.

⁵⁴⁴ For the full details of the decision see the Fine Issued for Infringements of the GDPR in Mobile Application "Karantinas" (public sector, 12 thous. Eur; private sector, 3 thous. Eur) State Data Protection Inspectorate, <https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20App%20Karantinas.pdf> (accessed on 23 June 2024).

⁵⁴⁵ See The Fine Issued for Infringements of the GDPR in Mobile Application "Karantinas" (public sector, 12 thous. Eur; private sector, 3 thous. Eur) State Data Protection Inspectorate, <https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20App%20Karantinas.pdf> (accessed on 23 June 2024).

application's privacy policy.⁵⁴⁶ Similarly, another example on this one was that Polish Data Protection Supervisory Authority (UODO) sent a letter to the Ministry of Digital Affairs indicating a few issues in relation to the contact tracing app ProteGo Safe, particularly relating the lack of clarity on the legal basis of the processing activities, as according to UODO, permission is the sole legal justification for processing user data.⁵⁴⁷ It chastised the program for failing to inform its users of the data handled in a trustworthy manner in advance.⁵⁴⁸ As for risk of transparency and legal basis risk delineated in Chapter 2, the indication of the legal basis of the processing is provided by the privacy statements of the data controllers must be thorough and error-free.

Having said that, we believe that it is not sufficient by itself. There should be consistency and unity among transparency, legal basis, and accountability of the controller. In other words, what is not elaborately addressed in the existing literature is that there is also the need to identify the role of any other third-party service providers, not to cause to such ambiguity as described in the above-mentioned case investigated by the Lithuanian DPA, to fully and properly comply with legal basis requirements. Also, Spanish DPA (AEPD) reiterated the requirements that must be met for personal data processing to be legal.⁵⁴⁹ The grounds that legitimize/make such processing possible are

⁵⁴⁶ See The Fine Issued for Infringements of the GDPR in Mobile Application “Karantinas” (public sector, 12 thous. Eur; private sector, 3 thous. Eur) State Data Protection Inspectorate, <https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20App%20Karantinas.pdf> (accessed on 23 June 2024).

⁵⁴⁷ See Liberties, Decisions and Recommendations of Data Protection Authorities in Europe: Knowledge Hub: Covid-19 Applications in the EU, Poland Section <https://www.liberties.eu/en/stories/trackerhub2-dpa-decisions/43529> (accessed on 23 June 2024), and for the full decision see PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH (in Polish) <https://bip.brpo.gov.pl/sites/default/files/Odpowied%C5%BA%20PUODO,%2019.06.2020.pdf> (accessed on 20 June 2024)

⁵⁴⁸ See Liberties, Decisions and Recommendations of Data Protection Authorities in Europe: Knowledge Hub: Covid-19 Applications in the EU, Poland Section <https://www.liberties.eu/en/stories/trackerhub2-dpa-decisions/43529> (accessed on 23 June 2024).

⁵⁴⁹ See the statement of Agencia Española de Protección de Datos <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad> (available in Spanish) (accessed on 23 August 2022).

the need to attend to the missions carried out in the public interest, as well as the need to guarantee the vital interests of those affected or of third parties.⁵⁵⁰ Accordingly, as elaborated on in Chapter 1, the data controller of the Spanish Radar Covid application built its lawful basis on protecting and safeguarding an essential interest for people's lives, in addition to the consent,⁵⁵¹ which will be detailed in Chapter 6. Having said that, these examples, regarding the efficient mutual implementation of legal basis and transparency requirements could be varied. For example, similarly data controller of the Belgium contact tracing applications indicated the legal basis on the grounds of public interest in the area of public health (9.2 (i) GDPR).⁵⁵² Or differently, data controller of the Finland contact tracing application did also state its legal basis of the processing by stipulating in their privacy statement that the processing of personal data is always based on valid legislation.⁵⁵³ Similarly, France's application aligned the legal basis of processing with Article 6.1.e of the GDPR,⁵⁵⁴ while the Netherlands' application⁵⁵⁵ indicated processing based on a public duty, whereas many EEA countries, especially Germany,⁵⁵⁶ and Estonia,⁵⁵⁷ explicitly delineated the nature of transactions tied to collected consents and highlighted the option for data subjects to immediately revoke their consents upon request within the framework of the legal basis of processing, as extensively outlined in Chapter 1.

Therefore, in summary, from our perspective, what is crucial to emphasize is that irrespective of the chosen legal basis, there should be a conspicuous and

⁵⁵⁰ See the statement of Agencia Española de Protección de Datos <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad> (available in Spanish) (accessed on 23 August 2022).

⁵⁵¹ Radar Covid, Privacy Policy, op.cit., Section 4, para 3.

⁵⁵² Corona Alert, Privacy Statement, op.cit., Section 3, para 1.

⁵⁵³ Koronavilkku Privacy <https://koronavilkku.fi/en/privacy/> (accessed on 22 January 2023).

⁵⁵⁴ Tous Anti-Covid Privacy, op.cit., Legal Basis and Regulatory Nature of the Processing Section

⁵⁵⁵ Corona Melder, Privacy Policy, op.cit., Section 3.

⁵⁵⁶ Corona Warn, Privacy, op.cit., Section 3, para 1 and Section 12, para 1.

⁵⁵⁷ HOIA Phone Application Privacy Policy, op.it., Section 7, para 1, and Section 13, para 1

consistent alignment between the selected legal basis for processing within digital contact tracing activities and their communication to data subjects. This unity ensures the consistent fulfilment of GDPR requirements.⁵⁵⁸ Such requirement also reiterated by the German Data Protection Authority⁵⁵⁹, which reiterated that the apps' transparency is critical for the acceptance rate, or similarly Slovenian Data Protection Authority⁵⁶⁰ opined on the requirement for transparency for the implementation of the applications.⁵⁶¹ The aforementioned sampled countries, among others, chose diverse lawful bases for processing activities, yet they effectively linked their chosen legal basis to meet the transparency requirement, ensuring clarity and understanding. Therefore, each of the recommended actions in the Transparency section is necessary to reinforce the indication of the lawful basis as well.

Consequently, the most crucial step to establish this lawful basis is to clearly specify and indicate the chosen basis. This part of the compliance activities creates the main challenge for data controller of contact tracing activities based on our detailed research. As said, it is crucial to establish a precise method for specifying these legal bases and consistently adhering to them throughout the entire lifecycle of processing activities, underscoring its immense significance. As proposed by us, sending regular SMS and emails related to any change that effects legal basis of processing activities, or any

⁵⁵⁸ See Article 13 of the GDPR, Information to be provided where personal data are collected from the data subject.

⁵⁵⁹ For the full statement of Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (German Data Protection Authority), see *Datenschutz bei Corona-Warn-App ausreichend* (in German) https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/12_Corona-Warn-App.html (accessed on 22 June 2024).

⁵⁶⁰ For the full opinion of Informacijski pooblaščenec (Slovenian Data Protection Authority) see *Opinions prior to the application of the General Regulation (before 25.5.2018)*, *Mnenja pred začetkom uporabe Splošne uredbe (pred 25.5.2018)* (in Slovenian) https://www.ip-rs.si/vop?tx_jzgdprdecisions_pi1%5BshowUid%5D=1504 (accessed on 23 June 2024).

⁵⁶¹ See Liberties, *Decisions and Recommendations of Data Protection Authorities in Europe: Knowledge Hub: Covid-19 Applications in the EU, Slovenia Section* <https://www.liberties.eu/en/stories/trackerhub2-dpa-decisions/43529> (accessed on 23 June 2024).

need for update in consent-based transactions must be prioritized by data controllers. Furthermore, such updates must be transmitted to the third-party data processors, to provide the consistent implementation across the entire chain of processing activities in terms of applicability of legal basis. By this method, it is possible to mitigate the risks related to arbitrary and inconsistent application of lawful basis of processing by data controllers and processors. Having said that, from our perspective, there is another issue regarding the amount of type of legal basis. This is delineated by Bradford, and colleagues as well, who mentioned that data controller needs only one lawful basis in each of Articles 6 and 9 as a 'floor', but it might choose to go above the floor.⁵⁶² For instance, a public health authority might process data through applications to safeguard the public from infectious diseases. The GDPR permits such processing within specific, multi-dimensional limits that may differ from an individual's personal view of what constitutes appropriate protection.⁵⁶³ Indeed, we concur with their view that multi-dimensional limits, in particular within the field of contact tracing applications, could be confusing for users and there is a likelihood that it sometimes differs from what a data subject deems appropriate protection.

To take a step further, what we propose is, as it is not elaborately addressed in the existing literature, the best way to address this ambiguity could involve identifying a primary dominant legal basis outlined in Article 6 and 9 of the GDPR. Users of contact tracing applications could be informed about this primary legal basis, alongside other pertinent information that needs to be communicated to users. This method aims to offer clarity amidst potential ambiguity. As clearly stated by the ICO, in case there is a real change in circumstances or data controller have a new and unanticipated purpose that means there is a good reason to review its lawful basis and make a change, it will be necessary that data controller will inform the individual and document

⁵⁶² Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes." *Journal of Law and the Biosciences*, vol. 7, no. 1, Isaa034, pp.1-21, p.12.

⁵⁶³ *Ibid.*

this change.⁵⁶⁴ Accordingly, we think that the sample is related to Smittestop application of Norway, whose use was banned by the Norwegian Data Protection Authority⁵⁶⁵ on temporary basis, is a great exemplification of such situation, as briefly delineated in Chapter 1. In more detail, due to the Norwegian Institute of Public Health's (NIPH) failure to show the app's benefits, Norwegian authorities have temporarily banned the processing of personal data using the Smittestop application.⁵⁶⁶ Additionally, they discovered that the NIPH had not satisfactorily demonstrated why using GPS position data for contact tracing was necessary, which they believe is in violation of the data minimization principle. Thus, the data controller may suppose that more than one basis applies; in this case, the controller should recognize and record each basis right away.⁵⁶⁷ Correspondingly, from our perspective, this decision clearly indicated to us that further consideration required for the evolving nature of contact tracing activities and needs arising from these efforts. Hence, it is beneficial to rely on document the necessity of contact tracing with supporting technical justification from the beginning, and in case there is any legal basis appears, it is important to justify it with these supporting documents and clearly indicate the users and explain what has changed and why are the reason of such change and potential outcomes those changes on the rights and freedoms of the data subjects. Accordingly, this justification via supporting documentation and notification might be

⁵⁶⁴ See ICO (2023), "Lawful Basis for Processing" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (accessed on 23 June 2024).

⁵⁶⁵ See Datatilsynet (the Norwegian Data Protection Authority), Temporary suspension of the Norwegian Covid-19 contact tracing app <https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/> (accessed on 20 June 2024).

⁵⁶⁶ For the full statement of Norwegian Data Protection Authority, see Datatilsynet, Temporary suspension of the Norwegian Covid-19 contact tracing app <https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/> (accessed on 20 June 2024).

⁵⁶⁷ See ICO (2023), "Lawful Basis for Processing" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (accessed on 23 June 2024).

achieved by controllers via detailed documentation available via layered notices as detailed under the notice and transparency requirements section 2.4. That said, it is crucial to consider the interaction between the lawful basis for processing and data subject rights, as outlined by Seinen and colleagues. They compared the two main mechanisms for further processing: consent and compatibility. Some data subject rights, such as access requests, the right to restrict processing, and the right to rectification, are independent of the lawful processing grounds⁵⁶⁸ for these rights, it does not matter whether consent or compatibility is the mechanism for further data processing.⁵⁶⁹ However, the exercise of other data subject rights, including the right to erasure, the right to data portability, and the right to object to processing, depends on the lawful ground of the initial processing. The issue of how these data subject rights are affected discussed in detail, as part of their work ⁵⁷⁰, which we find quite useful for our discussions as well.

As such, from our perspective, as for the data controllers of contact tracing applications, to the extent that those risks are applicable, they must be wary of any sort of malfunction related to the exercise of data subject rights. In other words, although there is less likelihood of facing a massive difference in the initial lawful basis of the processing activities for data controllers of contact tracing applications, regularly informing data subjects with regards to the drastic changes is of massive importance for complying with the data subject rights stipulated under the GDPR⁵⁷¹. Considering the nature of pandemics that last way less than business activity, we think that it is important to renew such safeguards more often than other data processing undertakings or

⁵⁶⁸ Seinen, Wouter; Walter, Andre and van Grondelle, Sari (2018) "Compatibility as a mechanism for responsible further processing of personal data." *Annual Privacy Forum*, pp. 153-171. Springer, Cham, p.158.

⁵⁶⁹ Seinen, Wouter; Walter, Andre and van Grondelle, Sari (2018) "Compatibility as a mechanism ...", *op.cit.*, p.158.

⁵⁷⁰ For the full section see Seinen, Wouter; Walter, Andre and van Grondelle, Sari (2018) "Compatibility as a mechanism ...", *op.cit.*, p.158, section Data Subjects- Rights and Freedoms.

⁵⁷¹ Article 12 to 23 of the GDPR, data subject rights.

applications and perform the utmost care to protect the users' fundamental rights.

Therefore, considering these concrete samples, our evaluation on the topic is that the interplay between the legal basis of processing activities taking place within the scope of contact tracing activities and transparency mechanism, thereby privacy statement of the controllers is visible. As much as it is important to determine the right legal basis stipulated under Article 6 and 9 of the GDPR, it is also crucial to indicate such basis to the data subjects and the supervisory authorities. As per the above, considering that the legal basis is limited, as legitimate interest of the data controller, *inter alia*, is not applicable, selection of the correct legal basis does not constitute a challenge to data controllers, considering both samples in Chapter 1 and herein. However, indicating the legal basis as well as the clear description of the controller with the notices is still of great importance to the increased trust of users, thereby augmenting the amount of usage of contact tracing applications. To this end, each data controller of the contact tracing applications employed within the EEA is obliged by the GDPR to act as per this requirement by applying cutting-edge notification and transparency mechanisms to their users. As a good sign of compliance by the data controllers of EEA countries, each of them performed their indication of lawful basis, while some of them are more in line with our stance by providing more elaborate approach as detailed above. This method is not only crucial for the implementation of the legal basis, but also to document the justification of new legal basis arising in the future. Contact tracing applications employed within the EEA are putting an effort to do that based on their privacy policies as well as terms and conditions of the use. However, there is always a chance to solidify these mechanisms in light of the following sections, by considering the novelties brought by technologies and nature of the infectious disease at stake, increasing the amount of consent for the different features and data processing activities of the application. Hence, this method will solidify the reliability of contact tracing applications from the risk-based perspective.

2.2 Data Minimization

Data minimization principle, among other things, absolutely, holds significant importance in the development of innovative COVID-19 fighting solutions.⁵⁷² European jurisprudence specifically highlights the necessity to adhere to criteria like necessity, proportionality, and data minimization in the use of contact tracing applications.⁵⁷³ Accordingly, as outlined in Article 5 of the GDPR, personal data should be adequate, relevant, and restricted to what is essential for the purposes they are processed for.⁵⁷⁴ Furthermore, data controllers are also required to mitigate the risks elaborated in Chapter 2 in Data Management and Architecture of the Applications sections in their processing activities by using data minimization practices. In other words, data processing entities collect data from subjects only to the extent necessary to achieve their processing objectives,⁵⁷⁵ and the amount of data that is subject to processing or exchange by contact tracing applications must be diminished to a strict minimum.⁵⁷⁶ For example, as mentioned in Chapter 2, asking about the users' favourite places to visit or the identity of their close friends would cause a breach of the data minimization principle,⁵⁷⁷ since it is not directly related to contact tracing activities. Likewise, another example of the reflection of data minimization on the apps, as known, the applications have been vastly developed by the national or country lead health

⁵⁷² Alessandra Pierucci, Jean-Philippe Walter (2020) “*Joint Statement on Digital Contact Tracing...*”, op.cit. p.3.

⁵⁷³ Vergallo, Ginaluca Montanari; Zaami, Simona; Bruti, Valerio; Signore, Fabrizio and Marinelli, Enrico (2021) "The COVID-19 pandemic and contact tracing technologies, between upholding the right to health and personal data protection", *European Review for Medical and Pharmacological Sciences*, vol.25, no. 5, pp.2449-2456, p.2452.

⁵⁷⁴ Article 5 of the GDPR, Principles relating to processing of personal data.

⁵⁷⁵ See European Commission Website, GDPR Principles https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en (accessed on 15 August 2022).

⁵⁷⁶ Ventrella, Emanuele (2020) “Privacy in emergency circumstances: data protection and the COVID-19 pandemic”, *ERA Forum* 21, pp. 379–393 <https://doi.org/10.1007/s12027-020-00629-3>, p.387.

⁵⁷⁷ Article 5-1-c of the GDPR, principles relating to processing of personal data, data minimization.

regulators.⁵⁷⁸ In order to provide a reliable and efficient decision, the developed applications use the information from different smartphone sensors i.e. GPS and Bluetooth, along with names, addresses, gender, age, contact details, calling log history, contact history, and so forth to render the decision.⁵⁷⁹ Therefore, although from the technical point of view, as described in Chapter 1, centralized applications are more closely linked with authorities, users are more likely to be required to hand over their personal data.⁵⁸⁰ ,whereas decentralized applications implement data minimization principles and require no user registration as core functions are built into the app,⁵⁸¹ it does not give us a clear cut answer on the best implementation of data minimization principle. The reason is that these applications either interact automatically with the national health data system pertaining to the test results of the citizens or the citizens could manually provide test results to the health organization.⁵⁸² To this end, the applications employed within the EU process the individual's symptom data, data about vaccination status, and location data, each of which must be carefully analysed from the data minimization perspective⁵⁸³, by understanding the sub-components of data minimization principle under the GDPR.⁵⁸⁴

⁵⁷⁸ Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2020) "A first look at privacy analysis of COVID-19 contact-tracing mobile applications", *IEEE Internet of Things Journal* 8, no. 21, pp. 15796-15806., p.15798.

⁵⁷⁹ Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2020) "A first look...", *op.cit.*, p.15798.

⁵⁸⁰ Vuokko, Riikka; Saranto, Kaija and Palojoki, Sari (2021) "Features of COVID-19 applications and their impact on contact tracing: results of preliminary review", *Finnish Journal of eHealth and eWelfare*, vol.13, no. 4, pp. 347-359, p.352.

⁵⁸¹ Vuokko, Riikka; Saranto, Kaija and Palojoki, Sari (2021) "Features of COVID-19...", *op.cit.* p.352.

⁵⁸² *Ibid.*

⁵⁸³ See European Commission Website, Mobile Contact Tracing Apps https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (accessed on 23 June 2024).

⁵⁸⁴ Article 5-1-c of the GDPR, principles relating to processing of personal data, data minimization.

Accordingly, first, it is important to perceive the nuances of data minimization requirements, rather than focusing on the amount of data collected, as sometimes advertised by many practitioners⁵⁸⁵⁵⁸⁶⁵⁸⁷. The principle of data minimization, by its nature, aims to establish a clear link between the personal data collected by data controllers and the purposes for which data are collected.⁵⁸⁸ We believe that data controllers must consider this clear link during the processing activities.

To be more specific, as advised by the ICO for the proper implementation of the data minimization, data controllers must ensure the personal data they are processing should be sufficient to properly fulfil the stated purpose, have a rational link to that purpose, and not be more than they need for that purpose.⁵⁸⁹ From our perspective, what can be achieved by data controllers is establishing a set of processing scenarios to be simulated that oblige the application to adhere to the strict minimum rule and clear linkage requirement. By utilizing these scenarios, any vulnerabilities of data processing activities that lead to a breach of the data minimization principle could be displayed. Considering these scenarios, we also believe that data minimization requirements and the required links with purposes for which data are collected could be strictly embedded in the privacy-by-design process. Accordingly, as a facilitator for this goal, the interplay between the DPIA and privacy-by-

⁵⁸⁵ See Jeirussen, Simone (2021) "Why Less is More When it Comes to Data?" Towards Data Science, <https://towardsdatascience.com/why-less-is-more-when-it-comes-to-data-8b90619fdeaf> (accessed on 23 June 2024).

⁵⁸⁶ See Zumbrun, Josh, (2022) "When it comes to data sometimes less is more", The Wall Street Journal <https://www.wsj.com/articles/when-it-comes-to-data-sometimes-less-is-more-11667554203> (accessed on 23 June 2024).

⁵⁸⁷ For further information see PricewaterhouseCoopers (PWC) (2020) "In the era of data protection, less data is more" <https://www.pwc.ch/en/publications/2020/In%20the%20era%20of%20data%20Protection.pdf> (accessed on 23 June 2024)

⁵⁸⁸ Galdón-Clavell, Gemma; Zamorano, Mariano Martín; Castillo, Carlos; Smith, Oliver and Matic, Aleksandar (2020) "Auditing algorithms: On lessons learned and the risks of data minimization", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 265-271, p.266.

⁵⁸⁹ ICO (2023), "Principle C- Data Minimization", <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> (accessed on 23 June 2024).

design/default strategies must be leveraged to the design of data minimization linkages for each processing case scenario. With the help of this set of processing scenarios simulated in DPIAs to find the riskiest part of any processing activity, the collection of personal data will be minimized, albeit within the context of what data is required by the controller to accomplish its data processing goals.⁵⁹⁰

In addition, identifying the sub-components of the term "health data" is crucial for applying the principle of data minimization, and therefore, it is necessary to specify the types and justifications for the information requested by contact tracing applications.⁵⁹¹

Specifically, we would like to refer to the questions that were asked regarding the symptoms of Covid-19, for example, high fever, malaise, joint pain, etc. While it is appropriate in terms of minimizing the collected data, it would not be appropriate to collect health data that is irrelevant to this purpose at stake. For example, a question about whether there is a chronic disease will suffice, while asking about non-chronic diseases or asking the details of the chronic disease will not be of primary importance. In other words, the term "strict minimum personal data" should not be stretched to encompass all healthcare-related information, as "health information" is too broad.

To be more indicative, for example, as detailed in Chapter 1, the efficient sample is the statement of the Norwegian contact tracing application⁵⁹² on the data minimization matters by specifying the type of each data processed⁵⁹³, whose detailed explanation was provided in Chapter 1. However, what is

⁵⁹⁰ Galdón-Clavell, Gemma; Zamorano, Mariano Martín; Castillo, Carlos; Smith, Oliver and Matic, Aleksandar (2020) "Auditing algorithms: ..." *op.cit.*, p.266.

⁵⁹¹ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p.387.

⁵⁹² See the archived Privacy Policy of Smittestopp, Section 4 <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy/> (accessed on 15 August 2022).

⁵⁹³ For the full description see the archived Privacy Policy of Smittestopp Section 4 <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy/> (accessed on 15 August 2022).

interesting about the Norwegian app's data minimization practice is that the Norwegian DPA finds these processing activities in breach of data minimization requirements,⁵⁹⁴ as briefly mentioned in the previous section. Although, based on their privacy policy and other related documentation, there is a positive implementation of data minimization requirements, in line with the GDPR requirements⁵⁹⁵, still there are some parts of the implementation, regarding the processing of location data, as indicated by the Norwegian Data Protection Authority, which triggers the data breach under the GDPR article. We find the decision of the Norwegian Data Protection Authority quite useful to understand the importance of the application of the data minimization principle through all the features of contact tracing applications. The reason is although the data controller meticulously contemplated the least use of data amount, it failed as it did not apply the same logic to the location data. To be more specific, it is evident that unrelated or unnecessary data, such as communication IDs, messages, civil status, equipment directory entries, call logs, location data, device identifiers, and so forth, should not be collected by any program.⁵⁹⁶ In which circumstances the application demands the use of a centralised server, the data being subject to processing by that server should be limited.⁵⁹⁷ Therefore, the Norwegian application, with a centralized processing model, acted accordingly and paid attention to the processing requirements.⁵⁹⁸ Nevertheless, from a legal perspective, once the data controller fails to adhere to one single requirement of the GDPR, it still remains "non-compliant" with the related GDPR requirement, regardless of the number of steps missed out on. Therefore, data

⁵⁹⁴For the full description and decision see Datatilsynet (the Norwegian Data Protection Authority), Temporary suspension of the Norwegian Covid-19 contact tracing app <https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/> (accessed on 20 June 2024).

⁵⁹⁵ Article 5-1-a and 5-1-e of the GDPR, transparency and storage limitation principles.

⁵⁹⁶ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p.387.

⁵⁹⁷ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p.387.

⁵⁹⁸ ICO COVID-19 Contact tracing: data protection expectations on app development available at: <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf>, p.3.

minimization practices require the end-to-end application across the entire set of data at stake, to fulfil the requirement under the GDPR⁵⁹⁹, and data controllers of the applications must act suitably. This approach namely “end-to-end compliance” with the data minimization requirements are, therefore, essential for data controllers, not to leave any single piece of personal data out of the data minimization practices.

Subsequently, another nuance of the data minimization requirement as elaborated in Chapter 2, is related to the fact that many smartphone applications also ask for unnecessary permission that is not required for the functionality of the applications, these apps might pose a serious threat to the privacy and security of the users⁶⁰⁰. To be more specific with the example, according to the Commission, symptom checks and telemedicine do not require access to the device owner's contact list if the functionality's intended use is for these reasons. Less data is produced and processed, which reduces security threats. As a result, following data minimization requirements also offers safeguards.⁶⁰¹ Thus, permitting the contact tracing apps to access further data in personal mobile phones must also be arranged as per the strict minimum principle by the controllers. Based on our interpretation it means that regardless of the architectural design of the apps, they should not need any data other than what is entered manually by the user data subject. Therefore, from our perspective, there is a requirement for a strict distinction between the required data for achieving the contact tracing purpose and technical necessities, which do not engage in personal data processing in any way. For instance, using the Bluetooth feature of a mobile phone would then fall into the latter category. The practical advantage of this distinct separation is eliminating any potential unintended excessive data processing by the controllers during the ask for technical permissions. Information on users'

⁵⁹⁹ Article 5-1-c of the GDPR, principles relating to processing of personal data, data minimization.

⁶⁰⁰ Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2020) “A first look...”, *op.cit*, p.15798.

⁶⁰¹ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).

proximity to one another can and should be collected without processing location data.⁶⁰² As such, health data should only be collected when absolutely necessary and on an optional basis, specifically for contact follow-up purposes, which means it should be used solely to assist in deciding whether to inform application users of potential exposure.⁶⁰³ To be more specific, as advised by the ICO, backend infrastructure should only collect identifiers after the user has taken a voluntary action, and should only process identifiers for the time needed to inform other users.⁶⁰⁴ In other words, data in server logs must be minimized in line with data protection law (i.e. no identifiers should be included).⁶⁰⁵

As a legal contribution to the technical implementation of the data minimization model, we strongly believe that this ambiguity regarding the permissions and artificial needs for further processing could be remediated by employing a strict opt-in mechanism for the data which has secondary importance for contact tracing activities, just as delineated in the consent requirement section in detail. In short, when users want to adjust these settings, they should actively choose to opt-in and modify the settings themselves. For instance, if they wish to share more of their personal data with others, they should take deliberate steps to do so.⁶⁰⁶ However, it is also important to balance the minimization practices with the efficiency requirements of contact tracing activities. In other words, at the first glance, although opt-in methodology seems to be the safest way of implementing data minimization principle, due to increased level of user power on the amount of

⁶⁰² Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).

⁶⁰³ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p387.

⁶⁰⁴ ICO COVID-19 Contact tracing: data protection expectations on app development available at: <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf>, (accessed on 23 June 2024), p.10.

⁶⁰⁵ *Ibid.*

⁶⁰⁶ Calzolaio, Simone (2016) "Digital (and privacy) by default. Constitutional identity of e-government." *Giornale di Storia Costituzionale*, vol.31, pp.185-206.

data processed. On the other hand, as discussed by Tene and Polonetsky, the data protection principles must be balanced towards additional societal values, i.e., public health, national security and law enforcement etc.⁶⁰⁷ In which the situations the benefits of any potential data utilization evidently outweigh privacy risks, the legitimacy of processing should be assumed, even if data subjects reject to consent.⁶⁰⁸

We, accordingly, believe that this leads us to a highly important determination of the limits of stretching data minimization requirements set out under the GDPR⁶⁰⁹, given that so far, we addressed the components of data minimization practices of the applications, but did not address the limits of data minimization requirements. In other words, to address the grey areas, we need to perceive the potential loopholes resulting from the dilemma between more use of personal data against less privacy protection. For example, analysing Big Data for statistical purposes to analyse pandemic trends could be demanded by the data controllers within the scope of processing activities, considering that Big data would enable the use of advanced data analysis to filter out false positives and improve the estimation.⁶¹⁰ Subsequently, data subjects (users) could simply reject opting into such analysis, as it should be, at the first glance. Nevertheless, if it was related to using of Big Data, thereby further consideration of this principle would be required as it would potentially undermine the success of Big Data initiatives as stated by Tal Z. Zarsky.⁶¹¹ However, the fundamental purpose of contact tracing applications, as discussed in the previous section, is to tackle the spread of Covid-19 pandemic and thereby processing personal data for

⁶⁰⁷ Tene, Omer, and Polonetsky, Jules (2011) "Privacy in the age of big data: a time for big decisions." *Stan. L. Rev. Online* 64, pp.63-69, p.67.

⁶⁰⁸ *Ibid.*

⁶⁰⁹ Article 5-1-c of the GDPR, principles relating to processing of personal data, data minimization.

⁶¹⁰ Maccari, Leonardo, and Cagno, Valeria (2021) "Do we need a contact tracing app?", *Computer Communications*, vol. 166, pp. 9-18, p.16.

⁶¹¹ Zarsky, Tal Z. (2016) "Incompatible: The GDPR in the age of big data", *Seton Hall L. Rev.*, vol. 47, pp. 995-1020, p.1011.

only sending warnings to the impacted users, rather than implementing big data analysis. With efficiency of the applications in mind, some of the controllers, as per the EU data, such as Italy, Germany, Netherlands, France, Finland, Spain and Norway applications used the data analysis sourced from multiple sources, such as from user surveys, applications' backend components, and other various methods for efficiency measuring and statistical purposes.⁶¹² However, not all controllers implemented this approach.

Accordingly, returning to challenges of such big data analysis, for instance, software developers have difficulties in satisfying data minimization requirements when they could not pre-determine the benefits large-scale data analysis could bring into the system.⁶¹³ Therefore, developers tried to expand the principle of data minimization requirements across the complete data processing chain within the application (collection, storage, and sharing) to minimize using user data in the system. Also, developers were inconsistent in the areas they focused on (collection, storage) and the techniques they used (encryption, aggregation) to implement data minimization requirements in their system designs.⁶¹⁴

As such, as seen this may lead to the abuse of the data minimization as well as storage limitation principles, whereas the distinction between a general use-case and contact tracing purposes may contain many different aspects due to its public health concerns. To put it differently, although we do agree with the necessity of discussing the balance and benefits to public health when assessing the contact tracing applications, as also mentioned by the other scholars in the literature, still it will remain open to abusive practices by data controllers for the further processing or storing by using cutting-edge

⁶¹² For the full data see European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", op.cit., p.62 - p.67.

⁶¹³ For the full article see Senarath, Awanthika, and Arachchilage, Nalin Asanka Gamagedara (2018) "Understanding software developers' approach towards implementing data minimization." *arXiv preprint arXiv:1808.01479*, pp.1-4, p.4.

⁶¹⁴ *Ibid.*

means of technological tools. Therefore, we consider that to strike the most optimal balance between the stretch of the limits of data minimization and public health, EU regulatory actors, in conjunction with the European Cybersecurity Agency⁶¹⁵, should step in to provide case-by-case analysis following to Covid pandemic. Within this regard, Tene and Polonetsky, also reiterated the importance of policymakers in addressing the role of consent in the privacy framework.⁶¹⁶ However, we believe that conducting a case-by-case analysis and disclosing the results will facilitate a comprehensive approach to evaluating the data minimization requirement alongside other GDPR mandates. In other words, other aspects of data protection compliance that influence effective data minimization—such as data protection impact assessments, privacy by design, and privacy by default—are addressed in the following sections. Therefore, it is possible to have a holistic view pertaining to the implementation of the principles set out under the GDPR, which we consider in line with the spirit of the regulation. In short, neither using a strict opt-in mechanism, nor stretching the limits of the data minimization principle for the sake of public health would resolve the data minimization dilemma. Hence, it requires regulators to step in with an approach, on which both benefits are agreed.

We are of the view that both for architecture of the applications and legal activities of applications, the EDPB should identify certain binding ground rules, although they have already published some sources to help data controllers and users, thereby society, still there is a need to issue certain binding ground rules for contact tracing applications, which will be examined in Chapter 5. Accordingly, as part of these aforementioned ground rules, with

⁶¹⁵ As per the European Union Agency For Cyber Security Website “The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.” <https://www.enisa.europa.eu/> (accessed on 3 March 2023).

⁶¹⁶ Tene, Omer, and Polonetsky, Jules (2011) "Privacy in the age of big data: a time for big decisions." *Stan. L. Rev. Online* 64, pp.63-69. p.67.

regards to consistency in implementing the measures to achieve data minimization and storage limitation for contact tracing applications, it is beneficial to have a standardized contact tracing approach as also put forward by Piergiuseppe Di Marco and colleagues⁶¹⁷ that proposed a system architecture for contact tracing based on the Bluetooth mesh standard and addressed challenges and opportunities for its adoption in critical facilities. Also, they advocated for standardizing Bluetooth mesh models that include configurable parameters for contact tracing purposes⁶¹⁸. We find their perspective on standardizing Bluetooth mesh models is in line with the spirit of evolving nature of contact tracing activities from privacy preserving perspective, as supported above. Moreover, standardizing Bluetooth mesh models might potentially increase the level of security of processing as in line with the article 32 of the GDPR. Standardizing the process might also cover the other aspects of contact tracing applications. Nevertheless, more than that, what we aspire to focus on is to the term of “standardization” for the most crucial features of contact tracing applications to comply with data minimization and storage limitation principles, rather than only one single technical aspect.

Within this respect, we find the view of Mbunge⁶¹⁹ regarding standardized contact tracing approach applicable to digital contact tracing activities is remarkable. As per his offer, these contact tracing apps are custom-made and not standardized globally, which means each country develop contact tracing app that has its Internet of Things infrastructure, devices, APIs, and data formats leading to interoperability issues.⁶²⁰ As such, interoperability issues

⁶¹⁷ For the entire proposed solutions refer to Di Marco, Piergiuseppe; Park, Pangun; Pratesi, Marco and Santucci, Fortunato (2021) "A Bluetooth-Based Architecture for Contact Tracing in Healthcare Facilities", *Journal of Sensor and Actuator Networks*, vol.10, no. 2, pp.1-15. <https://doi.org/10.3390/jsan10010002>.

⁶¹⁸ Di Marco, Piergiuseppe; Park, Pangun; Pratesi, Marco and Santucci, Fortunato (2021) "A Bluetooth-based architecture...", *op.cit.* p.14.

⁶¹⁹ For the entire proposed solutions refer to Mbunge, Elliot (2020) "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol.14, n. 6, pp. 1631-1636.

⁶²⁰ Mbunge, Elliot, (2020) "Integrating emerging technologies...", *op. cit.* p.1634.

involve various factors, such as differences in networking standards and communication protocols, variations in data semantics and ontology, diverse data formats, different operating systems, and multiple programming languages, among other elements.⁶²¹ Data formats and structure should be standardized across all platforms to avoid incomplete and noisy data, thereby improving data quality. Standardization process is also backed by a few scholars in the field, with the different components. For instance, Marhold and Held investigate multi-mode standardization process of contact tracing apps during the COVID-19 pandemic.⁶²² Their research shows that the market cannot solve standardization problems under time pressure. Governments should therefore create standard-setting policies for future crisis situations.⁶²³ We are sharing the same perspective as them by adding that most of the problematic aspects in terms of data minimization standards could be dealt with elaborately by the regulator. Although, as the EDPB and Commission published guidance, which will be detailed in Chapter 5, still there is room for further development in the field. It is obviously not a straightforward task to consider each disaster scenarios in terms of the overstretch or abuse of data minimization principle, as detailed above, and come up with a clear-cut solution. Therefore, this standard approach must be aligned with privacy-by-design perspective, which will be analysed in Chapter 4. Nevertheless, as a positive sign of compliance, regardless of their architectural choice of processing, centralized or decentralized, each of the data controllers, implemented a unified approach, and react quick to such unexpected and rare situation.

Correspondingly, to conclude, even though many of the data controllers endeavour to reflect data minimization requirements under the GDPR and ePrivacy directive onto their contact tracing activities, as discussed, there are

⁶²¹ Mbunge, Elliot, (2020) "Integrating emerging technologies...", *op. cit.*, p.1634.

⁶²² For the full article see Marhold, Klaus, and Fell, Jan (2022) "Multi-mode standardization under extreme time-pressure—the case of COVID-19 contact-tracing apps." *R&D Management*, vol. 52, no. 2, 356-375.

⁶²³ *Ibid.* p.368.

still some nuances to address such as the interplay between the purpose and limited amount of data, or similarly the standardized data minimization practices across Europe, not to give unfair treatment to any of the European citizens. In the following sections, we will further deep dive into the other data processing principles set out under the GDPR and ePrivacy Directive, to complement the data minimization approach from a holistic perspective, as many of which go hand in hand.

2.3 Purpose Limitation

The purpose limitation principle, inter alia, is set out under the article 5 of the GDPR⁶²⁴, which creates an obligation for data controllers by stipulating that processing data should only occur when it is essential within the framework of a particular transaction.⁶²⁵ Similarly, data controllers are also required to mitigate the risks elaborated in Chapter 2 under Data Management and Architecture of the Applications sections in their processing activities. Moreover, the ePrivacy Directive extensively addressed the collection of location data, highlighting the potential high privacy risks, particularly when tracking individuals' movement patterns.⁶²⁶ Consequently, concerning contact tracing efforts, the primary aim of data processing is to curb the spread of the Covid-19 pandemic within the community. Thus, European data controllers are obliged to gather each piece of data in alignment with this specific purpose. Therefore, within the context of contact tracing activities, the purpose of the data processing activity is to prevent the spread of the Covid-19 pandemic in the community. In this context, each data to be processed by the data controller must be collected in accordance with this purpose by the European data controllers. Purpose limitation preserves data subjects by determining limits on the use of their personal data by data controllers while

⁶²⁴ Article 5 of the GDPR, purpose limitation principle.

⁶²⁵ See European Commission Website, GDPR Principles, Purpose https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing_en (accessed on 15 August 2022).

⁶²⁶ Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021). "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps", *Empir Software Eng*, vol.26, pp. 1-51, <https://doi.org/10.1007/s10664-020-09934-4> p.20.

at the same time offering a level of room in terms of flexibility for data controllers.⁶²⁷

Correspondingly, the principle of purpose limitation has two key components: personal data must be collected for "specified, explicit, and legitimate" purposes (purpose specification), and it must not be "further processed in a way incompatible" with those purposes (compatible use).⁶²⁸ Determining the purposes from the outset enables data controllers to be accountable for their processing, and assists them to refrain from 'function creep'.⁶²⁹ It also assists users of contact tracing apps to understand how data controllers use their data, make decisions about if they are glad to share their details, and claim their rights over their data where needed, and thereby is fundamental to building public trust for a controller in the way it collects personal data. To this end, we can call out the fact that as per the EU Commission report, and independent review, other than the German, Italian, French, Ireland and Slovenian app, almost none of them opted for adding other functions such as management of vaccine and/or test certificates to the contact tracing applications, therefore, rest of the apps were not required to differentiate between the purposes.⁶³⁰ Furthermore, with regards to additional capabilities and functionalities, i.e. anonymized statistical analysis and etc., as per our review, it is possible mention that, while most of the apps in EEA/EU including

⁶²⁷ Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation Adopted On 2 April 2013, p.3.

⁶²⁸ Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation Adopted On 2 April 2013, p.3.

⁶²⁹ See ICO (2023), "Purpose Limitation" https://ico-org-uk.translate.google.com/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/?x_tr_sl=en&x_tr_tl=tr&x_tr_hl=tr&x_tr_pto=op.sc#limitation_principle (accessed on 23 June 2024).

⁶³⁰ For the full report see European Commission Digital Contact Tracing Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic VIGIE 2021-0649 Framework Contract SMART 2019/0024, Lot 2 available at: <https://commission.europa.eu/system/files/2023-02/DigitalContactTracingStudy.pdf> (accessed on 28 April 2024).

Germany, France, Ireland, Belgium, Italy and Slovenia⁶³¹ delineated the detailed of such purposes based on their privacy policies, some of the applications did not provide detailed information around the further activities with different purposes, i.e. statistical analysis, such as Austria, Latvia, Denmark⁶³² and etc. Accordingly, we believe that there is a room for further methodologies considering the complexities that might be created by pandemic in terms of varying purposes, given that pandemic might oblige controllers to add different purposes to the tool in the future. Therefore, we will deep dive into the nuances of potential solutions.

We, first, believe that the most secure approach for contact tracing apps involves setting up a system where data controllers or processors can solely process the personal data of individuals in society for a clearly specified purpose before engaging in any data processing activities.⁶³³ It is the most optimal option in the ideal world of data protection and privacy. Nevertheless, it is always not that much realistic to implement such an approach with a unified implementation across the entire EEA countries. Therefore, we would like to offer, the second-best alternative, whose implementation is more realistic and feasible. This corresponds to the fact that the notion of purpose limitation should be interpreted in a very narrow and limited manner, so as not to face any sort of incompliance risk.⁶³⁴ Fundamentally, Bluetooth location where needed, phone number of users for SMS notifications regarding security measures such as two-way authentication for logging into the application, and Covid-19 symptoms specific health data could be exemplified. Purposes must be clearly defined to prevent the misuse of these tools for other purposes, which means ensuring that apps cannot be repurposed for commercial or law enforcement activities unrelated to

⁶³¹ For the full details on other purposes delineated see Corona Warn app, op.cit. section 6, Immuni app op.cit., Section “analytics”, Tous Anti Covid app., op.cit, section “Data controller and purpose”, Coronaalert app. op.cit. section 3, HSE op.cit. section “personal data”.

⁶³² For the full details on other purposes delineated see the Stop Corona App, op.cit, section 4.9, Apturi Covid op.cit, section 1, Smittestop op.cit, section “for what purpose can my data be used?”.

⁶³³ Article 29 Data Protection Working Party (2013) Opinion 03/2013, *op.cit.*, p.3.

⁶³⁴ *Ibid.*

managing the COVID-19 health crisis.⁶³⁵ Therefore, as contact tracing applications evolve to incorporate new features, it is important to continuously reassess the associated privacy risks.⁶³⁶

The monitoring of compliance with quarantine and confinement measures, or the overall drawing of conclusions on the location of the user, should be excluded from the available purposes of digital contact tracing applications.⁶³⁷ Monetizing purposes, i.e., advertising, are not classified as necessary and therefore need to be based on another legal ground. Likewise, using data to create new features and services does not meet the specificity required by this section.⁶³⁸ To address this, data controllers of contact tracing applications must adhere to stringent guidelines from the outset, as outlined in the 'privacy-by-design' section of Chapter 4. In addition, a limited, narrow, and strict approach regarding the purpose of the processing activities implemented by data controller is key to the success of the compliance efforts. Although in the real world, there are plenty of examples, which could incentivize data controllers to easily ramble from the original purpose of processing, we believe that the narrower and stricter the definition of the purpose is, the less the of the GDPR requirements⁶³⁹ will occur. Having said that, to be more realistic and pragmatic for the solutions presented, we believe that the most problematic aspect in terms of purpose limitation perception of the controllers is to processing users' data with another purpose. The reason is, this principle creates a two-part test: the initial step involves specifying a lawful and explicit purpose for collecting the data, while any subsequent processing for another

⁶³⁵ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p.387.

⁶³⁶ *Ibid.*

⁶³⁷ *Ibid.*

⁶³⁸ Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021) "A privacy and security analysis...", *op.cit.*, p.12.

⁶³⁹ See Article 5-1-b of the GDPR.

purpose must align with and not contradict the original intention, as stated.⁶⁴⁰ Big data causing issues to the principle of purpose limitation, often seen as a barrier hindering the advancement of big data analytics.⁶⁴¹ The outlined critical aspects regarding purpose specification limitation notably hinder the effectiveness of the "notice and consent" model. For example, big data analytics enable data analysis using many different algorithms which reveals unexpected correlations that can be used for new purposes. Therefore, as per the approach of Andreu-Perez and colleagues, the purpose limitation principle restricts an organization's freedom to make these discoveries and innovations. In addition to repurpose, big data analytics also has the potential to create a new personal data. With the ability to deal with large volumes of both structured and unstructured data from different sources, big data analytical tools hold the promise to study outcomes of large-scale population-based longitudinal studies, as well as to capture trends and propose predictive models for data generated from electronic medical and health records.⁶⁴²

We partially can utilize the perspective brought by the authors for the legal analyse of contact tracing applications. The reason is that considering the main purpose of contact tracing activities is to tackle the infectious disease by warning people, the statistics or analyse related purpose by big data is therefore of secondary importance from the privacy perspective. We, thus, strongly recommend data controllers of contact tracing apps to treat statistics as a second important purpose of contact tracing activities to comply with the main component of the purpose limitation principle under the GDPR. It is also important to mitigate the risks associated with the use of the apps detailed in Chapter 2, regarding preventing any secondary use of personal data obtained

⁶⁴⁰ Colin Barker, (2014) "Big data must operate within data protection law," says watchdog, "and here's how", ZDNET. <https://www.zdnet.com/article/big-data-must-operate-within-data-protection-law-says-watchdog-and-heres-how/> (accessed on 19 November 2023).

⁶⁴¹ Ghani, Norjihhan Abdul; Hamid, Suraya and Udzir, Nur Izura (2016) "Big data and data protection: Issues with purpose limitation principle", International Journal of Advances in SoComputing & Its Applications, vol. 8, no. 3, pp.116-121, p.119.

⁶⁴² Andreu-Perez, Javier; Poon, Carmen CY; Merrifield, Robert D.; Wong, Stephen TC. and Yang, Guang-Zhong (2015) "Big data for health." *IEEE journal of biomedical and health informatics* 19, no. 4 pp. 1193-1208, p.1194.

by user data subjects. Moreover, the creation of new personal data from big data analytics requires us to provide an approach to get consent from data subjects towards their new personal data.⁶⁴³ In big data analytics, data collected for one purpose can often be repurposed in ways that greatly benefit society. The reason is, Big Data is most challenging, dynamic, heterogeneous, interrelated, and untrustworthy, even noisy Big Data could be more valuable than slight samples as general statistics received from frequent patterns and correlation analysis mostly overpower individual fluctuations and usually disclose more reliable hidden patterns and knowledge.⁶⁴⁴

We are of the view that the logic provided by the research of Norjihhan Abdul Ghani and colleagues could be beneficial for contact tracing applications aspect of purpose limitation requirements in this case scenario, considering that data processed by the applications could be subject to different purposes than initially collected. It is always safer to rely on stricter purpose limitations by sticking with the main purpose of processing, namely tracing the contacts of infected people in the society, unless data subject users provide their explicit consent beforehand for the further use of processed personal data. Hence, in case controllers face challenges with the claims brought by data subjects with a basis that they did not provide their consent for the new purposes as the new purpose is compatible with the original purpose, as stipulated under the GDPR.⁶⁴⁵ Nevertheless, we believe that in reality, as we understand based on our aforementioned research most of the European data controllers of contact tracing applications rely on public interest rather than consent mechanism, they must scrutinize the term “compatible use” detailed

⁶⁴³ Ghani, Norjihhan Abdul; Hamid, Suraya and Udzir, Nur Izura (2016) "Big data and data protection..." *op. cit.* p.119.

⁶⁴⁴ Agrawal, Divyakant; Bernstein, Philip; Bertino, Elisa; Davidson, Susan, Dayal, Umeshwas; Franklin, Michael; Gehrke, Johannes; Haas, Laura; Halevy, Alon; Han, Jiawei; Jagadish, H.V.; Labrinidis, Alexandros; Madden, Sam; Papakonstantinou, Yannis; Patel, Jignesh; Ramakrishnan, Raghu; Ross, Kenneth; Shahabi, Cyrus; Suciu, Vaithyanathan, Shiv; and Widom, Jennifer (2011) *Challenges and opportunities with Big Data*, Purdue University (Purdue e-Pubs), Cyber Center Technical Reports, 2011-1, p.1-16, p.6.

⁶⁴⁵ See Recital 50 of the GDPR, further processing of personal data.

by the Article 29 Working Party.⁶⁴⁶ Furthermore, we also consider that the scope of technology proves to be a real challenge for data controllers to distinguish between the main purpose and the secondary purpose. In other words, although in the ideal world, it must be easy to classify the purpose of the processing as pandemic related or not, given that both the pandemic and the type of technology evolves, the study of Kung and Martin,⁶⁴⁷ establishes a new perspective regarding the importance of privacy-enhancing-technologies, which we consider as a significant tool for engineers and developers of contact tracing applications as well. As per their approach, privacy-enhancing technologies keep being unknown by most engineers, because of the uncoupling between the Privacy-Enhancing Technologies and the practice of systematic engineering and development that makes engineers unaware or unknowledgeable of the proper applicability of such solutions.⁶⁴⁸ In practice, when engineers need to face privacy issues, they resort to crafting tailored solutions (in case any), rather than opt-in for the systematic and economic application of current solutions drawn from the state of the technique.⁶⁴⁹

Accordingly, from our perspective, contact tracing activities could be inevitably subject to further purposes of processing during the lifecycle of contact tracing applications. For instance, as discussed, AI, aided by real-time data analysis, can offer updated information crucial for disease prevention.⁶⁵⁰ It could be instrumental in predicting potential infection sites, anticipating virus spread, assessing bed and healthcare professional requirements amid this crisis.. AI is helpful for future virus and disease prevention, with the help of previous

⁶⁴⁶ See Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation, p.21.

⁶⁴⁷ For the full article see Martin, Yod-Samuel, and Kung, Antonio (2018) "Methods and tools for GDPR compliance through privacy and data protection engineering." In 2018 IEEE European symposium on security and privacy workshops (EuroS&PW), IEEE, pp. 108-111.

⁶⁴⁸ Martin, Yod-Samuel, and Kung, Antonio (2018) "Methods and tools for GDPR....", op.cit., p.108.

⁶⁴⁹ *Ibid.* p.108.

⁶⁵⁰ Vaishya, Raju; Javaid, Mohd; Khan, Ibrahim Haleem and Haleem, Abid (2020) "Artificial Intelligence (AI) applications for COVID-19 pandemic", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp 337-339, p.339.

mentored data over data prevalent at different times. Likewise, bundling of functionalities within the same application (e.g., a single app providing general information, symptom checker features, and contact tracing) or, should that be the case, clearly distinguish those functionalities and grant users granular control over which of them, they wishes to opt-in to.⁶⁵¹ Similarly, as mentioned by the WHO, solutions built using the decentralized architecture would be limited in their capacity for public health analysis, which means that health authorities may be required to employ alternative approaches (such as data donation or surveys) to enable information to be collected for different indicators.⁶⁵² Therefore, in light of these real-life examples regarding purposes of contact tracing processing, it is plausible to state that there is not one clear-cut classification of the main purpose of processing and further processing activities, which also disrupts the compatibility test proposed by WP. Nevertheless, to overcome such difficulties in the classification of initial and secondary purposes, we agree with the perspective that any processing after data collection, whether for the purposes initially determined or for any additional purposes, must be regarded “further processing” and must therefore fulfil the requirement of compatibility.⁶⁵³ This perspective could mitigate the ambiguity between the lines of initial purpose and secondary purpose as detailed above. According to the Working Party's perspective, assessing each situation individually is necessary to decide whether additional processing for a different purpose aligns with the initial intent.⁶⁵⁴ A

⁶⁵¹ *Ibid.*

⁶⁵² WHO, (2020) “Indicator framework for the evaluation of the public health effectiveness of digital proximity tracing solutions”, ISBN 978-92-4-002835-7 (electronic version), p.3.

⁶⁵³ For the full article See Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation Adopted On 2 April 2013 00569/13/EN WP 203, p.21 available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (accessed on 15 August 2022).

⁶⁵⁴ See Hunton Andrews Kurth, (2020) “Article 29 WP clarified purpose limitation principle on big and open data”, Hunton Privacy Blog available at: <https://www.huntonprivacyblog.com/2013/04/09/article-29-working-party-clarifies-purpose-limitation-principle-opines-on-big-and-open-data/> (accessed on 22 June 2024).

detailed compatibility assessment needs an evaluation of all relevant situations.⁶⁵⁵

Thus, we also recommend the compatibility test, guided by the WP29, which could be either formal or substantive.⁶⁵⁶ A formal assessment will compare the purposes that were initially provided, usually in writing, by the data controller with any further uses to find out whether these uses were covered (explicitly or implicitly). A substantive assessment involves more than just formal declarations; it involves recognizing both the new and original purposes, understanding how they are perceived (or should be) in various contexts and considering additional factors, depending on the context and other factors. While the first method may, at first sight, seem more objective and neutral, it risks being too rigid and building too much on formal text. We believe that doing so, may encourage controllers to specify the purpose in increasingly more legalistic ways, with aim of allowing room for additional data processing rather than to protect the individuals concerned.⁶⁵⁷ The second method is more flexible and pragmatic, but also more effective: it may also enable adaptation to future developments within the society while at the same time continuing to safeguard the protection of personal data effectively. As a useful sample to support our perspective, we can consider the decision of the Spanish Data Protection Authority. As per the decision, the Spanish AEPD fined Equifax 1 million Euros for processing publicly available personal data unlawfully, in violation of the purpose limitation and other GDPR requirements.⁶⁵⁸ Equifax was instructed to halt the processing and remove all personal data that had undergone such processing.⁶⁵⁹ In question

⁶⁵⁵ *Ibid.*

⁶⁵⁶ See Article 29 Data Protection Working Party (2013) Opinion 03/2013 On Purpose Limitation, *op.cit.*, p.21.

⁶⁵⁷ *Ibid.*

⁶⁵⁸ For the full decision see AEPD, Procedimiento N°: PS/00240/2019 available at: <https://www.aepd.es/documento/ps-00240-2019.pdf> (accessed on 15 June 2024).

⁶⁵⁹ AEPD, Procedimiento N°: PS/00240/2019 available at: <https://www.aepd.es/documento/ps-00240-2019.pdf> (accessed on 15 June 2024).

is data Equifax acquired from the Spanish Official State Gazette, and different releases and debtors lists from other public bodies such as the General Tax Administration and city councils' gazettes, and accommodated in its File on Judicial Complaints and Public Bodies, obtained via public sources. In its most basic form, the purpose limitation principle states that personal information obtained for one purpose may not be utilized for another.⁶⁶⁰ As such, it defines the limits on how data controllers may use personal information, if a data controller chooses to change these boundaries and use data for purposes that were not reasonably envisaged by the data subject at the time of collection, it must notify the data subjects and, at the very least, inform them of the new purposes, which is in line with our proposed approach for the contact tracing applications to mitigate any abuse or ambiguity.

Therefore, in conclusion, designing an application that does not cause any vulnerability within the scope of the GDPR requirements from the beginning is the key component of the purpose limitation.⁶⁶¹ Through this approach, contact tracing applications can perform their tasks by staying within the boundaries in terms of purpose selected by the data controllers prior to processing activities. As mentioned in Chapter 1, as a result of our review, each of the contact tracing applications within Europe seem to put an effort to clearly set out their intention of following the purpose limitation by indicating a “specified, explicit and legitimate” purpose as in line with Article 29 WP Opinion⁶⁶² that provided guidance to the application of the GDPR principles. As mentioned, there was not any application skipping this requirement as all of them provided this purpose in either privacy policy or terms of use somehow. This is a positive sign about the prevention of any potential risks to rights and freedom of data subject rights, as prescribed by the Recital 75 of

⁶⁶⁰ See Williams, John and Cohen, Bret (2020) “What does the CCPA's 'purpose limitation' mean for businesses?” IAPP, <https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses/#:~:text=Background,controllers%20may%20use%20personal%20information> (accessed on 15 June 2024)

⁶⁶¹ Article 12 to 23 of the GDPR. data subject rights.

⁶⁶² Article 29 Data Protection Working Party Opinion 03/2013, *op.cit.*, p.3.

the GDPR.⁶⁶³ That being said, irrespective of any gap identified, once there will be further capabilities to use in a single application, our proposals detailed here will surely contribute to data controllers enhancing their purpose limitation practices, as they feasible alternatives, considering potential usage for different purposes in the future.

2.4 Consent Requirement:

Consent is required, inter alia, with other legal basis, to process personal data and special categories of personal data as per the article 6 and the article 9 of the GDPR and composes an important element of data processing activities as detailed in the Chapter 1. Data protection regulations enacted in many countries oblige undertakings to obtain user consent before starting any data collection activities.⁶⁶⁴ Likewise, data controllers are also required to mitigate the risks elaborated in the Chapter 2 under Data Management, Localisation Data and Obligation of Use the applications sections in their processing activities. In most Member States, "consent" is given primary importance for lawful data processing, as emphasized in Recital 30 of the Directive, which is considered the main condition for processing data.⁶⁶⁵ However, in some Member States, "consent" is just one of several possible criteria for data processing, or it is to be relied upon only as a last resort.⁶⁶⁶ Even in data protection's most legitimizing provision as a fundamental right, Article 8 of the Charter of Fundamental Rights of the European Union (the Charter), consent is enshrined as an alternative for the bases of fair processing.⁶⁶⁷

Therefore, pertaining to the consent requirement, as the contact tracing applications process, among others, sensitive data, there must be either clear

⁶⁶³ Recital 75 of the GDPR, Risks to the Rights and Freedoms of Natural Persons.

⁶⁶⁴ Trivedi, Ameer; Zakaria, Camellia; Balan, Rajesh; Becker, Ann; Corey, George and Shenoy, Prashant (2021) "WiFiTrace: Networkbased Contact Tracing for Infectious Diseases..." *op.cit.*, p.6.

⁶⁶⁵ Ferretti, Federico (2014) "Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?", *Common Market Law Review*, vol.51, no. 3, pp.843-868, p.846.

⁶⁶⁶ *Ibid.*

⁶⁶⁷ Zafir, Gabriela (2014) "Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law", *Reloading Data Protection*, Springer, Dordrecht, pp. 237-257, p.239.

consent or the existence of one of the other legal bases stipulated under the GDPR.⁶⁶⁸ The processing of personal data to implement tracing applications within the scope of the pandemic constitutes the legal basis of the data processing activity. The provisions of article 5⁶⁶⁹ and 6⁶⁷⁰ of the GDPR set out that the necessary conditions must exist for the processing of personal data other than the consent of the person. However, it is not possible to apply the same logic for a special category of personal data, given that a special category of personal data⁶⁷¹ must be predominantly processed with the consent of the person themselves. Personal data, other than the special category of personal data, on the other hand, can be processed for the purposes mentioned in both article 6(1)(d) and (e)⁶⁷² of the GDPR⁶⁷³. While the first legal basis allows processing personal data, which is required to protect the legitimate interest of individuals, namely saving their lives, the second one can be used to protect public interests or when exercising official authority provided to the controller.⁶⁷⁴

Nonetheless, as detailed in Chapter 1 and the legal basis of processing part of Chapter 3, most of the contact tracing applications rely on public interest as a legal basis of processing. Therefore, it is indicated in Chapter 1 that the consent mechanism is not prioritized by the data controllers, as it is more difficult to collect and time-consuming for data controllers. Having said that, consent is still preferred by the data controllers for disclosure of the data of

⁶⁶⁸ Article 9 of the GDPR, processing of special categories of personal data.

⁶⁶⁹ Article 5 of the GDPR, principles.

⁶⁷⁰ Article 6 of the GDPR, lawfulness of processing.

⁶⁷¹ As per the Article 9/1 of the GDPR "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

⁶⁷² Article 6 (1) (e) of the GDPR, already mentioned.

⁶⁷³ Article 6 (1) (d) of the GDPR stipulates that processing is required to safeguard the vital interests of the data subject or another individual.

⁶⁷⁴ Ventrella, Emanuele (2020) "Privacy in emergency circumstances...", *op.cit.*, p.381.

the users.⁶⁷⁵ It is also used for some specific features of the applications, for instance, some apps, including but not limited to Croatia⁶⁷⁶, Germany⁶⁷⁷, Spain⁶⁷⁸, Lithuania⁶⁷⁹, Austria⁶⁸⁰ utilized consent for only certain features such as installation, activation of GAEN notifications or Bluetooth technology, exposure logging and etc. In the parallel vein, Slovenian application, for instance, relied on opt-out consent by obliging data subjects to disable certain features in case they do not want to log their exposure.⁶⁸¹ Also, it is used for the sharing of their infected keys with third countries via the European interoperability platform, thus facilitating the digital tracing of potential close contacts.⁶⁸² Nevertheless, the room for consent use in practice is strictly limited to these specific cases in practice, and we will delineate the other significant aspects related to contact tracing activities.

First, from our perspective, considering the urgency of the situation, relying on a consent mechanism for contact tracing application processing would not be in line with the spirit of the GDPR and its interaction with the European conventions. In other words, implementation of lawful basis seems more realistic and efficient, when we consider finding the optimal implementation. The reason is that the privacy-first approach is stemming from one of the most fundamental rights of the EU citizens set out in the Convention. However, on the other hand, considering a situation where data subjects rely on customized consent, it would radically decrease the ease of processing of personal data by the controllers within the scope of contact tracing activities.

⁶⁷⁵ See archived Smittestopp Privacy Policy, Section 3 <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy/> (accessed on 11 August 2022).

⁶⁷⁶ Stop Covid-19 App privacy policy, op.cit. section 6.

⁶⁷⁷ Radar covid app privacy policy, op.cit. section 4.

⁶⁷⁸ CoronaWarn App privacy policy, op.cit. section 12.a.

⁶⁷⁹ Korona Stop LT Privacy Policy, op.cit. section 2.

⁶⁸⁰ The Stop Corona App privacy policy, op.cit. section 4.4.

⁶⁸¹ See Section 4 of the Privacy Policy of OstaniZdraw application, legal basis.

⁶⁸² See Radar Covid, Privacy Policy, op.cit., section 4

It seems like a plausible and desired scenario at the first glance, as it may provide further discretion over their personal data. Nonetheless, in case the other principles are implemented thoroughly to address the risks elaborated in Chapter 2, the consent mechanism would be of secondary importance for the efficient protection of data subjects. Correspondingly, if we just imagine what the Article 4(11) of the GDPR sets out for the consent of the data subject, which stipulates that consent must be any voluntarily expressed, specific, briefed, and unquestionable acknowledgement of the data subject's preferences,⁶⁸³ we could easily see the fulfilling more than one requirement is necessary to implement consent thoroughly, on the contrary to the general understanding. Thus, for instance, as a general principle, the GDPR stipulates that consent is considered invalid if the data subject lacks a meaningful selection, feels coerced into giving consent, or faces negative consequences for not consenting. Additionally, consent is deemed not to be freely given in case it is included as a mandatory part of terms and conditions.⁶⁸⁴ Current practice in terms of asking for consent expects the data subject to tick a box to ask for consent and offer a link to a privacy policy, this mechanism fails a number of GDPR regulations, including being explicit and specific.⁶⁸⁵ Accordingly, in case data controllers aspire to utilize consent for the contact tracing applications, they must rely on the indication of will from the data subject to the process prescribed personal data within the scope of tracking activities.

Furthermore, pertaining to the freely providing consent, any implicit enforcement of using the contact tracing applications to visit a country or to room in a specific country could damage the freely given consent, as there is an implicit obligation. Hence, data controllers must be diligent in setting out these obligations for data subjects. As provided by the study of Krehling, Leah,

⁶⁸³ Article 29 Working Party, (2018) Guidelines on Consent under Regulation 2016/679 (wp259rev.01), p.5.

⁶⁸⁴ *Ibid.*

⁶⁸⁵ Breen, Stephen; Ouazzane, Karim and Patel, Preeti (2020) "GDPR: Is your consent valid?", *Business Information Review*, vol. 37, no. 1, pp. 19-24, p.20.

and Aleksander Essex under the privacy principles of contact tracing, with regards to the proper disclosure and consent, users should be provided easy-to-understand information on the functions of the application and all data it uses and stores, therefore users must provide their consent to all data processing.⁶⁸⁶ In other words, Express consent is required at each stage of data sharing and must be meaningful, not buried behind lengthy privacy rules or unclear language agreements, and involves explicit consent to disclose COVID-19 test results anonymously.⁶⁸⁷ Therefore, it is not sufficient to obtain a simple affirmation, but also prior to this consent, there is a need for meticulously prepared notice, as detailed in Chapter 4. In addition to this, another problematic aspect is, considering Recital 4⁶⁸⁸, which clearly indicates that it is not really possible that public authorities could rely on consent for processing because each time the controller is a public authority, there is often a power imbalance in the relationship between controllers and data subjects. It is also clear that in many cases the data subject has no realistic alternative to accepting this processing (conditions) of the controller. Working Party 29 is of an opinion that there are other legal grounds that are, in principle, better fitting to the activity of public authorities.⁶⁸⁹ This is in line with the ideas presented in the 'Legal Basis' section of this Chapter. Having said that, without prejudice to these general considerations, it does not entirely preclude a public authority's use of consent as a justification for data processing within the GDPR legal framework. Therefore, as mentioned above, upon providing detailed information to the users, and allowing the users opt-in freely, to

⁶⁸⁶ Krehling, Leah, and Essex, Aleksander (2021) "A security and privacy scoring system for contact tracing apps", *Journal of Cybersecurity and Privacy*, vol.1, no. 4, pp. 597-614, p.601.

⁶⁸⁷ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy with public digital contact tracing during the COVID-19 pandemic", *Lancet Digit Health*, vol. 2, n.7, doi: 10.1016/S2589-7500(20)30133-3, pp e342-e344, p.e343.

⁶⁸⁸ In summary, Recital 43 of the GDPR indicates that to guarantee the voluntary nature of consent, it cannot serve as a lawful basis for processing personal data if there exists a significant imbalance between the data subject and the controller, especially when the controller represents a public authority. In such cases, it's improbable that consent was freely given, considering the overall circumstances of that situation.

⁶⁸⁹ Article 29 Working Party, (2018) *Guidelines on Consent*, *op.cit.*, p.6.

mitigate any potential ambiguity, data controllers can ask data subjects to tick a box for each type of data collected. Such a process should be provided on the downloaded application, following the registration. Within this context, opt-in mechanisms delineated by the WP 29 within the scope of marketing activities could provide a context to the consent mechanism under contact tracing applications, although their purpose of processing differs massively.⁶⁹⁰ Arguably, several tactics can be used to build and sustain public trust in such applications.⁶⁹¹

Thus, we believe that in order to establish a solid consent mechanism, cutting-edge methods and easier consent mechanisms must be developed by the data controllers as per the WP 29 guidance.⁶⁹² To be more clear, explicit consent at each step of data sharing is crucial and must be meaningful, not embedded into lengthy privacy policies or massive language agreements, and contains explicit consent to anonymously share COVID-19 test results. When individuals are given the chance to consent to the use of their personal data as a fundamental way to exercise their autonomy and safeguard their privacy, it is reasonable to also offer them the option to withdraw, revoke, or amend that consent in the future.⁶⁹³ Within this logic of the GDPR, its reflection on contact tracing applications could be implemented via tailor-made smart contracts, which self-enforce the terms of the contract when the pre-determined conditions are triggered.⁶⁹⁴ A party "signs" a smart-contract with cryptographic security and deploys it on a distributed ledger or

⁶⁹⁰ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) 'The need for privacy...', *op.cit.* p.343.

⁶⁹¹ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) 'The need for privacy...', *op.cit.* p.343.

⁶⁹² Article 29 Working Party, (2018) Guidelines on Consent, *op.cit.*, p.9.

⁶⁹³ Politou, Eugenia; Alepis, Efthimios and Patsakis, Constantinos (2018) "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions", *Journal of cybersecurity*, vol.4, no. 1, pp. 1-20, p.5.

⁶⁹⁴ O'Shields, Reggie (2017) "Smart contracts: Legal agreements for the blockchain." *NC Banking Inst.*, vol.21, pp.177-194, p.179.

blockchain.⁶⁹⁵ Ahmed, and colleagues evaluated the consent withdrawal process at various stages of the app operation,⁶⁹⁶ which is in line with the perspective we brought as well. Their study classified the circumstances where revoke of the consent takes place. These circumstances are divided in three, namely data collection phase, data that is already uploaded to the server and end of pandemic era phase.⁶⁹⁷ The revoke of consent is theoretically should be as easy as to provide the consent, as prescribed under the GDPR⁶⁹⁸, which is also very important novelties brought by the GDPR. In line with this perspective, we believe that the study of the authors⁶⁹⁹, brought a useful perspective on smart contracts and consent revoking mechanism, whose underlying logic could be utilized for the contact tracing applications. In their study, they described a proposal for a blockchain-based GDPR-compliant personal data management platform, whose main objective is to provide a personal data usage control system for complying with the regulation's manifold legal requirements.⁷⁰⁰ Their proposed system consists of two smart contracts: the consent contract, which embodies the authorization given to a data controller from a data subject to collect his personal data for a period of time, and the purpose contract, which contains the permission given to a data processor to process a subset of data subject's

⁶⁹⁵ *Ibid.*

⁶⁹⁶ Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha. (2020) "A survey of COVID-19 contact tracing apps", *IEEE access*, vol. 8, pp.134577-134601, p.134596.

⁶⁹⁷ *Ibid.*

⁶⁹⁸ In summary of the consent withdrawal matter provided under the GDPR, Article 7-3 of the GDPR indicates that the data subject retains the right to revoke their consent at any moment, without this action impacting the legality of processing based on the consent given before its withdrawal. Before granting consent, the data subject must be duly informed about this possibility. The process of withdrawing consent should be as simple as giving it initially, ensuring ease of action for the individual.

⁶⁹⁹ The referred authors are Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha.

⁷⁰⁰ For the full article see Daudén-Esmel, Cristòfol; Castellà-Roca, Jordi; Viejo, Alexandre and Domingo-Ferrer, Josep (2021) "Lightweight blockchain-based platform for gdpr-compliant personal data management", 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), pp. 68-73, p.70.

personal data for a specific objective and for a limited period of time.⁷⁰¹ Additionally, their proposed system on 'revokeConsentPurpose' is quite useful as well. This method revokes the processing consent of all-purpose smart contracts, created from this Consent smart contracts, that have as purpose argument the one specified when calling this method. It also removes the specified purpose from the "defaultPurposes list" in case it is in there.⁷⁰²

As such, we believe that smart contracts, are an efficient tool, considering that their importance is becoming more visible in the last few months. The reason being is, smart contracts offer perceived benefits such as swifter and more accurate business transactions, increased operational efficiency, cost-effective contract enforcement, and the adaptation of legal principles to electronic transactions, potentially obviating the need for new laws or regulations.⁷⁰³ Correspondingly, it is plausible to acknowledge that considering the urgency of needs in pandemic scenario, implementing a consent mechanism via smart contracts method is actually in line with the spirit of the GDPR, in terms of the data controller obligations pertaining to the implementing cutting-edge and cost efficient solutions.⁷⁰⁴

From the same consent revoke perspective, although the presented solution is related to a blockchain platform, implementing an instant deletion of the processing consent from the servers could be in line with the spirit of the GDPR as described above. This assumption is subject to the limitations and the technical feasibility of the proposed system for contact tracing applications, which is not the main discussion of the thesis. However, from the regulatory perspective, implementing a consent revoke mechanism which is

⁷⁰¹ Daudén-Esmel, Cristòfol; Castellà-Roca, Jordi; Viejo, Alexandre and Domingo-Ferrer, Josep (2021) "Lightweight blockchain-based platform...", *op.cit.*, p.71.

⁷⁰² Daudén-Esmel, Cristòfol; Castellà-Roca, Jordi; Viejo, Alexandre and Domingo-Ferrer, Josep (2021) "Lightweight blockchain-based platform...", *op.cit.*, p.71.

⁷⁰³ O'Shields, Reggie (2017) "Smart contracts..." *op.cit.*, p.179.

⁷⁰⁴ Since Article 25 of the GDPR emphasizes the "the state of the art and the cost of implementation" for the implementation of appropriate technical and organizational measures, we are of view that the proposed approach would be in line with this perspective brought by the GDPR.

to be effective promptly upon the revoke of the consent, could be genuinely beneficial for data controllers of contact tracing applications, regardless of its nature or design. Organizations are required to take sufficient steps to manage revocation, and accordingly, organizations must cease any ongoing process instances that are impacted by the revocation.⁷⁰⁵ Furthermore, there is a lack of universal approach against smart contracts which could impede giving or revoking the consent, during the interoperable application of contact tracing applications. Hence, it is crucial to create and embrace universal smart contract languages and coding standards to avert coding mistakes and fraud while ensuring consensus and reliability⁷⁰⁶, to talk about such mechanism without any impediment.

Having said that, regardless of how advantageous of smart contracts in terms of revoking the consents, considering the workload and cost associated with the revoke, in line with the considerations of the GDPR, data controllers should consider the gradual consent mechanism. Nonetheless, from the legal point of view, to employ such a mechanism, the most crucial thing for a data controller is to have the technical capability for implementing the vital features bundled in the initial consent, and the respective steps for further processing of personal data which has secondary importance for the use of the application. It would perfectly fulfil the GDPR consent requirements⁷⁰⁷ and could create another cutting-edge solution for the controllers of the apps. For example, the methodology implemented for website cookie consents by many data controllers is shedding light onto the structure of our proposed consent mechanism. In the privacy notices, as seen in Chapter 1, the data protection measures, and the type of data processed are enumerated. Therefore, whereas the core data could be bundled for the initial consent collected from data subjects by the data controller, the subsequent consent could be strictly

⁷⁰⁵ Besik, Saliha Irem and Freytag, Johann-Christoph (2020) "Managing Consent in Workflows under GDPR", *ZEUS Workshop 2020*, in Manner, Johannes; Haarmann, Stephan; Kolb, Stefan; and Kopp, Oliver (eds.), CEUR Workshop Proceedings, n. 2575, pp. 18-25, p.19.

⁷⁰⁶ McKinney, Scott A.; Landy, Rachel and Wilka, Rachel (2017) "Smart contracts, blockchain, and the next frontier of transactional law", *Wash. JL Tech. & Arts*, vol. 13, pp.313-347, p.346.

⁷⁰⁷ Article 7 of the GDPR, conditions for consent.

tailored to every single piece of personal data processed. This approach could be leveraged for combining different lawful basis, i.e. relying on lawful basis other than consent and provide a room for consent for other processing activities or features as briefly mentioned in the first sub-chapter, as some of the controllers, such as Spain, Germany etc. has already tried to do as well. By this, both GDPR requirements would be perfectly satisfied in terms of cost efficiency and novelty of the solution, and user trust would be strictly enhanced, and can provide data controllers with efficient legal and technical solution for implementation of the consent mechanism.

To conclude, considering that all contact tracing applications employed within the GDPR jurisdictions rely on other legal bases for the major portion of the processing activities, i.e. preserving public health, as mentioned in the related section of this Chapter, realistically speaking, room for consent seemed to be limited for contact tracing applications. Thus, in case data controllers have a desire to rely on the consent of the users, above mentioned factors could play an important role to implement an efficient consent mechanism. From our perspective, relying on cutting-edge and thorough consent models is always more in line with the spirit of the GDPR and ePrivacy directive, within the scope of implementation of contact tracing applications. Contact tracing applications employed within the EEA put an effort to do that based on their privacy policies as well as terms and conditions of the use. However, there is a chance to solidify these mechanisms by considering more room for consent for each secondary portion of the processing activities by using the novelties brought by technologies within the field of consent management solutions, as detailed above.

2.5 Notice, Transparency and Accountability Requirement

Providing notice regarding type of data collected, for how long it is to be stored, for which purposes and by whom they are processed is of massive importance for mitigating several privacy related risks detailed in the Chapter 2, as well as the responsibilities under the GDPR compliance for Notice⁷⁰⁸,

⁷⁰⁸ Article 5-2 of the GDPR, principle of accountability.

Transparency⁷⁰⁹ and Accountability of the data controllers⁷¹⁰, as they are interpreted holistically in the data protection literature. The requirement to incorporate specific information in a privacy statement for GDPR compliance does not garner as much attention as other GDPR obligations, despite its necessity.⁷¹¹ However, it is of great importance in terms of preventing any potential conflicts between the data controllers of contact tracing applications and data subjects. Also, transparency is significant in circumstances where people can decide whether or not they want to engage with a data controller.⁷¹² Therefore, data controllers, in line with their transparency obligations, ought to make sure to avoid any misunderstanding as to what the applicable legal basis is.⁷¹³ As mentioned by Hobson, and colleagues, transparency of the technologies by an understanding of how every single addresses the concerns is a foundation for building trust and enabling stakeholders to make decisions about which technologies they want to use and how they want to use them.⁷¹⁴ Therefore, although explained in Chapter 1, most data controllers of the applications have extensive statements, there is still room for improvement for efficient compliance with the GDPR requirements, given that there is an ambiguity on identity of controller, missing information on details of third parties as well as on data protection officer, and some various aspects as well. We will not point finger to each potentially

⁷⁰⁹ Article 5-1-a of the GDPR, principle of transparency.

⁷¹⁰ Article 13 of the GDPR, Information to be provided where personal data are collected from the data subject.

⁷¹¹ Hintze, Mike (2018) "Privacy Statements under the GDPR", *Seattle UL Rev.*, vol. 42, p.1129-1154.

⁷¹² ICO (2023), Guide on Principle (a): Lawfulness, fairness and transparency <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> (accessed on 23 June 2024) Section 'What is Transparency' para. 2.

⁷¹³ EDPB (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (accessed on 15 August 2022) p.7.

⁷¹⁴ Hobson, Stacy, Michael Hind, Aleksandra Mojsilovic, and Kush R. Varshney (2020) "Trust and transparency in contact tracing applications", *arXiv preprint arXiv:2006.11356*, pp.1-9, p.4.

missing part in their privacy policies and other relevant documentations, as the term of missing is varying within the context of contact tracing. Instead, we will focus on what could be introduced as an enhancement, in line with the specific of digital contact tracing matters, as from our perspective, efficiently implementing transparency requirements within apps relies on various factors, including users' trust in the privacy and security of the application while they use it.⁷¹⁵

First, we believe that there is a clear link between the transparency and consent requirements under the GDPR and the ePrivacy directive.⁷¹⁶ Regarding what data controllers consider most, by the GDPR's definition the consent should be "freely given, specific, informed, and unambiguous"⁷¹⁷, as detailed in consent requirement section of Chapter 3. Accordingly, the information related to the processing activities of contact tracing apps shall be provided in writing, or by other means, as stated by the GDPR.⁷¹⁸ Having said that, it should be understandable and easy-to-perceive, to fulfil the information duty, while at the same time comprising as much detailed information as possible. In other words, while we wait for the development of such privacy-preserving applications, privacy policies indicating the risks associated with the use of contact-tracing applications are necessary, in a format that could

⁷¹⁵ Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha. (2020) "A survey of COVID-19 ..." *op.cit.* p.134584.

⁷¹⁶ See article 7 of the GDPR and Article 9-1- of the ePrivacy Directive.

⁷¹⁷ Recital 32 of the GDPR indicates that consent must be obtained through a clear, affirmative action demonstrating the data subject's voluntary, specific, well-informed, and unmistakable agreement to the processing of their personal data. This agreement could manifest as a written or electronic statement, or verbally. For instance, it might involve ticking a box on a website, adjusting technical settings for online services, or another action or statement clearly indicating the data subject's acceptance of their data being processed in that context. Silence, pre-selected options, or inactivity should not be considered as valid consent. Consent needs to encompass all processing activities performed for the same purpose(s), and if there are multiple purposes, consent must be granted for each. In cases where electronic means are used to seek consent, the request should be transparent, brief, and not unnecessarily disruptive to the service being provided.

⁷¹⁸ Article 5 of the GDPR, principles relating to data processing.

be straightforwardly read and understood by the public.⁷¹⁹ However, interestingly, there is not any clear-cut answer regarding the type and content of the notice in the EDPB Guideline. To this end, we strongly advise considering that applications might evolve with the changing nature of the pandemic. Every update to the notice should be communicated to the relevant individual via email and SMS, and consent for each new update should be consistently obtained. In other words, data controllers must ensure that the statement is "easily accessible," meaning it should be straightforward to locate from the outset.⁷²⁰ The privacy statement links must be placed on prominent and consistent areas across all points wherein an individual interacts with an organization, ensuring straightforward access and uniformity.⁷²¹ Otherwise, the access of the data subject that does not submit consent on updated terms should be temporarily suspended. According to ICO guidance, contact tracing app initiatives should clearly outline their goals, specifying whether the benefits primarily serve the user or have broader societal implications. Transparency about objectives, requirements, and future strategies is crucial for fostering trust among all stakeholders, particularly users.⁷²² Correspondingly, it's crucial to recognize that GDPR's stipulations on exercising data subject rights and the required information aim to empower individuals, enabling them to assert their rights and hold data controllers accountable for their personal data processing activities.⁷²³ Within this context, as demonstrated by the use of thermal cameras at Brussels Airport to establish if travelers had body temperatures of at least 38 degrees Celsius, the Belgian Supervisory Authority instigated an ex officio investigation against

⁷¹⁹ Zhang, Melvyn; Chow, Aloysius and Smith, Helen (2020) "COVID-19 Contact-Tracing Apps..." *op.cit.* p.2.

⁷²⁰ Hintze, Mike. (2018) "Privacy Statements..." , *op. cit.*, p.1151.

⁷²¹ Hintze, Mike. (2018) "Privacy Statements..." , *op. cit.*, p.1151.

⁷²² ICO COVID-19 Contact tracing: data protection expectations on app development available at: <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf>, p.5.

⁷²³ EDPB (2016) Guidelines on Transparency under Regulation 2016/679, *op. cit.*, p.7.

controllers in 2020.⁷²⁴ The decision made by the Belgian Supervisory Authority included several aspects among other considerations, a controller who lacked transparency with the data subjects infringed Articles 12 to 14 of the GDPR. The primary cause of this violation is that the controller's privacy statement omitted to mention the legal justification for the processing.⁷²⁵ Hence, as we can see clearly in this sample that contact tracing app privacy policies should offer transparency to data subjects regarding their rights outlined in Articles 12 to 23 of the GDPR before any processing occurs. Additionally, these rights should be highlighted through brief reminders sent as notifications to users' mobile phones whenever they log in. We consider this one a significant indicator of contact tracing applications as well. Among many other reasons to provide a detailed and clear privacy notice, the performance of data subjects' rights is quite crucial due to the European approach. On the positive side, in most countries, including, France, Germany, the Netherlands, Malta, Belgium, Lithuania, the Estonia, Republic of Cyprus, Slovenia, Ireland and Portugal, the primary promotion of the app occurred during its initial launch. Advertising efforts encompassed social media, television, radio, newspaper coverage, and press conferences aimed at medical professionals,⁷²⁶ which we believe is genuinely efficient tool to clearly convey the privacy message to the users to mitigate their concerns detailed in Chapter 2. Meanwhile, countries like Finland, Ireland, and Estonia integrated app promotion into broader strategies for combating the pandemic.

⁷²⁴ See EDPB Website, Summary of Decision on Temperature checks at Brussels Airport (Belgium) as part of the fight against COVID-19 Date of final decision 4 April 2020 https://edpb.europa.eu/news/national-news/2022/temperature-checks-brussels-airport-belgium-part-fight-against-covid-19_sv (accessed on 23 August 2022).

⁷²⁵ For the full decision see Gegevensbeschermingsautoriteit (Belgium Data Protection Authority), Beslissing ten gronde 48/2022 van 4 april 2022 Deze beslissing werd gedeeltelijk vernietigd ten aanzien van de eerste verweerder en geheel vernietigd ten aanzien van de tweede verweerder door het arrest 2022/AR/560&564 van het Marktenhof dd. 7 december 2022, (in Dutch) <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-48-2022.pdf> (accessed on 23 June 2024).

⁷²⁶ European Commission, Directorate-General for Communications Networks, Content and Technology, Prodan, A., Birov, S., Wyl, V. et al., Digital contact tracing study – Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2759/146050>, p.45.

For instance, the Finnish app Koronavilkku was one element among five in a elaborate multilingual campaign (Finnish, Swedish, and English) aimed at educating the public about key infection prevention measures, whereas in the Republic of Cyprus, Malta, France, and the Czech Republic, the government worked with mobile phone operators to send mass SMS messages to citizens, which included a link to download the app.⁷²⁷ We are of view that such creative solutions should be encouraged and diversified further so that it might create a solution in line with the realities of our new technology era.

Within this information context, what is not elaborately addressed in the existing literature is that this situation can be completed with a text that would be required to be read during the first registration phase of contact tracing applications. We believe including a concise section displaying data subjects' rights in a small, separate box within the submission text can significantly help address practical issues. Essentially, each application should offer a brief and clear one or two-page information and confirmation text, ensuring it's easily accessible, transparent, and understandable.⁷²⁸ Correspondingly, in line with our approach, regarding the content of the apps, as mentioned by Zhang M and colleagues examined the privacy policies of seven applications⁷²⁹ they concluded that these policies are deemed “very difficult” to read and comprehend for the majority of individuals.⁷³⁰ We do agree with this perspective, brought by Zhang for some of the European counterparts. Based on our research of the privacy policies, although they elaborated each future of contact tracing applications, which is really a useful feature though, most of

⁷²⁷ *Ibid.*, p.46.

⁷²⁸ Article 29 Working Party Guidelines on Transparency under Regulation 2016/679, *op. cit.*, p.7.

⁷²⁹ Zhang, Melvyn; Chow, Aloysius and Smith, Helen (2020) “COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies”, *Journal of medical Internet research*, vol.22, n.12,e21572, pp.1-6, in their study they investigated “the contents of the privacy policies of these apps were assessed for readability using Readability Test Tool, a free web-based reliability calculator, which computes scores based on a number of statistics (i.e., word count and the number of complex words) and indices (ie, Flesch Reading Ease, Flesch-Kincaid Reading Grade Level, Gunning Fog Index, and Simplified Measure of Gobbledygook index)”.

⁷³⁰ Zhang, Melvyn; Chow, Aloysius and Smith, Helen (2020) “COVID-19 Contact-Tracing Apps: Analysis of the...”, *op.cit.*, p.5.

them are provided with a complex structure and language, which must be subject to simplification.

From our angle, to mitigate such complexity, layered notices can play an important role in the design of these policies. As for this layered notice approach, there is a requirement for short notice, which is the top layer, offers a user access to the privacy notice's essential components.⁷³¹ A layered approach to privacy notices would make very simple notices readily available with links to more detailed notices. The complete notice, which is the bottom layer, fully addresses all nuances. The Article 29 WP/EDPB recommended a layered notice in its guidance on complying with the GDPR to meet the GDPR's requirements that privacy notices be easily accessible, understandable, and written in clear and plain language.⁷³² Within the scope of layered notices, keeping the notices updated and informing users about any updates to privacy policies is equally crucial. Hence, we believe that it is an efficient tool to mitigate most of the concerns mentioned in Chapter 2 regarding transparency and accountability risks. Accordingly, as per the Article 29 WP, in case of consent is provided via electronic means, granular and layered information can be a decent way of handling the dual requirements of being accurate and comprehensive while also being understandable.⁷³³ Having said that, data controllers must still be aware that it will be challenging to prove that the data subject conveyed informed consent unless the data controller can demonstrate that the concerned data subject accessed that information prior to giving consent when the identity of the controller or the purpose of the processing (and also is not clear from the very

⁷³¹ See IAPP Website, Layered Notice <https://iapp.org/resources/article/layered-notice/> (accessed on 23 June 2024).

⁷³² *Ibid.*

⁷³³ EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.0 Adopted on 28 November 20174 May 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, (accessed on 23 June 2024), p.22.

first the information layer of the layered privacy notice situated into more sub-layers).⁷³⁴

Therefore, controllers of the apps should pay attention to the most vital elements of informing data subjects set out under the GDPR and make these notices more visible to data subjects. Conducting monthly reviews of privacy policies within contact tracing apps necessitates informing data subjects through diverse channels, ensuring they are not only apprised of any modifications but also provided with comprehensive reasoning for these regular assessments, thus fostering transparency regarding the evolving nature of the application's operations. By this, it would be easier to solidify the compliance mechanism and the trust of users, as data controllers have an opportunity to display to the users, they are taking their duties resulting from the GDPR. To be more specific with the real-life example of trust, as discussed, it is essential to note that ultimately a degree of trust is required in the use of any mobile application.⁷³⁵ This includes trusting the controllers, developers, the independent test and verification team, the operators and owners of the service, and importantly, the companies providing essential components such as the mobile phone operating systems.⁷³⁶ For instance, in the case of Twitter, the Irish supervisory authority set out, among other things, the confirmation of Twitter International Company, based on its Privacy Policy of its status as the relevant controller for the personal data of Twitter users in the EU.⁷³⁷ Hence, as a reflection on contact tracing applications, privacy policies of contact tracing applications are undertaking significant roles to

⁷³⁴ EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.0 Adopted on 28 November 2017 4 May 2020, p.25.

⁷³⁵ Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha. (2020) "A survey of COVID-19 ..." *op.cit.* p.134597.

⁷³⁶ Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha. (2020) "A survey of COVID-19 ..." *op.cit.* p.134597.

⁷³⁷ For the full decision see Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, available at : https://edpb.europa.eu/sites/default/files/files/file1/edpb_bindingdecision01_2020_en.pdf, p 12.

determine many other things including the accountability of the relevant controller, or the exercise of data subject rights, which goes hand in hand with the transparent approach aimed by the GDPR. As such, to mitigate such risks, which are elaborated on in Chapter 2, considering the complex nature of contact tracing activities, it is advisable to implement efficient transparency and notice mechanisms in line with the Article 12 and 13 of the GDPR.⁷³⁸ The more data controllers can standardize this transparent approach, the better implementation of data subject rights, thereby user trust could be attained by data controllers.

Within the similar vein but a different field, Cranor mentioned added standardization notices benefit consumers.⁷³⁹ From our angle, there seems to be a clear advantage of standardized notices for data subjects such as gaining trust toward controllers, implementing a quick decision-making for download of these applications and exercising their rights as mentioned. Accordingly, they are also of the view that standardized notices facilitate comparisons and allow consumers to become familiar with the terminology and where to look to find types of information.⁷⁴⁰ An extremely simple privacy notice, perhaps in the form of an icon, is likely to appeal to most consumers in his words, and users in our words due to the nature of the use of apps. Moreover, they also supported the view that standard policy types could simplify privacy decision-making.⁷⁴¹ Therefore, data subjects who want to have detailed information about their privacy can rely on a detailed policy, whereas those who do not want to read a long land detailed privacy policy can benefit from the outline comprising the most important aspects of processing activities, in line with our layered notice approach. To support the importance of a standardized approach, for instance, we would also like to point out the findings of another

⁷³⁸ See Article 12 and 13 of the GDPR, Transparent information, communication and modalities for the exercise of the rights of the data subject, and Information to be provided where personal data are collected from the data subject.

⁷³⁹ *Ibid.*

⁷⁴⁰ Cranor, Lorrie Faith (2012) "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice", *J. on Telecomm. & High Tech. L.*, vol. 10, pp. 273-308, p.305.

⁷⁴¹ Cranor, Lorrie Faith (2012) "Necessary but not sufficient...", *op. cit.*, p.305.

study dealing with online privacy notices, which claim that current online privacy notices need to undergo a major reform if most consumers are to understand them.⁷⁴² This study provides objective measures to support prior consumer research, which found that consumers are frustrated with current privacy notices.⁷⁴³ Accordingly, privacy notices should be scored for readability standards to ensure that a significant proportion of the target population has the educational level needed to read the notices. To guarantee that a substantial portion of the intended audience possesses the necessary literacy level to comprehend the provided notices. Second, their data show that notices have increased in length. However, longer notices do not necessarily mean that the notice itself is more difficult to read. Both length and grade level should be considered in assessing notices.⁷⁴⁴ Accordingly, considering the trend of declining readability across different sectors, the necessity of having general standards are independent of industry sector can also provide a view on the structure of privacy notices created for contact tracing applications. In other words, controllers of the tracing applications can be better off by implementing a standard type of privacy notice. Employing this standard notice approach could entail, both successful fulfilment of transparency requirement under the GDPR by a standardization reform, as well as increased number of users of the application, thereby efficiency in tracking of cases. Having said that, even though this standardization of the information notices seems doable and easy at the first glance, considering that each application relies on a different technical infrastructure, it is not really considered without transforming each of the applications into one form. Indeed, to achieve such an end-to-end standard approach, the guidance and leadership of the EU Commission and the EDPB could be an important

⁷⁴² For the full article see Milne, George R.; Culnan, Mary J. and Greene, Henry (2006) "A longitudinal assessment of online privacy notice readability", *Journal of Public Policy & Marketing*, vol. 25, no. 2, pp. 238-249.

⁷⁴³ Milne, George R.; Culnan, Mary J. and Greene, Henry. (2006) "A longitudinal assessment...", *op.cit.*, p. 245.

⁷⁴⁴ Milne, George R.; Culnan, Mary J. and Greene, Henry (2006) "A longitudinal assessment...", *op.cit.*, p. 245.

contributor. By their initiative, the main components of notices could be listed. We believe that such a regulatory approach would positively correlate with the success of user freedom on his personal data. However, without taking a regulatory approach, it is almost impossible to create such common standard of the privacy notices. Therefore, although there is a massive increase in the need for standard and more readable privacy notices across many fields including contact tracing activities, it requires the alignment of data protection approach by each data controller in the EEA jurisdiction.

Finally, another important component of transparency and accountability compliance is the indication of the data processing protocol and other important details of the contact tracing applications, which would solidify the indication of the accountable act of the controller. As mentioned by the research of Alrawais and other authors, the data collected from users are a source of great concern to them, as the methods of collecting this data and its uses must be clear and fulfil the terms of privacy.⁷⁴⁵ Similarly, with regards to utilizing personally identifiable information in algorithms that assign risk scores or categories to individuals, and accordingly potentially caused algorithmic bias and error, providing code and datasets publicly accessible and ensuring it is subject to peer review and continuing to refine the model as further data become available.⁷⁴⁶ From our perspective, making code and datasets publicly available would be positively correlated with the gaining trust of the users and the entire society as in line with the transparency requirement under the GDPR, as also detailed in privacy-by-design section.⁷⁴⁷ In other words, to accomplish transparency, the full functionality of the mentioned

⁷⁴⁵ Alrawais, Arwa; Alharbi, Fatemah; Almoteri, Moteeb; Altamimi, Beshayr; Alnafisah, Hessa and Aljumeiah, Nourah (2022) "Privacy-Preserving Techniques in Social Distancing Applications: A Comprehensive Survey." *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol.26, n. 3, pp. 325-34, p.337.

⁷⁴⁶ For the full article and discussions see Mello, Michelle M., and C. Jason Wang. (2020) "Ethics and governance for digital disease surveillance." *Science* 368, no. 6494, pp. 951-954, p.953.

⁷⁴⁷ Article 5-1-a of the GDPR, lawfulness, fairness and transparency.

solution must be open source.⁷⁴⁸ It grants researchers and experts the chance of reviewing the privacy conditions applied by the proposed system and thus increases their confidence in it.⁷⁴⁹ Therefore governments, to enhance trust, should also declare that exactly that code is running, so any further holes can be checked and the whole functionality should be made open-source.⁷⁵⁰ On the positive side, as per the git hub sources, many controllers including but not limited to Italy⁷⁵¹, Czechia⁷⁵², Iceland⁷⁵³, Cyprus⁷⁵⁴, Poland⁷⁵⁵, Malta⁷⁵⁶ and the all others, other than Lithuania and Hungary.

From our perspective, this is quite in line with the approach to increase the privacy safeguards and reliability of the applications. It is also possible to use experts and specialists to review privacy procedures in the proposed solutions, which will maintain data privacy therein.⁷⁵⁷ Therefore, in order to determine certain risks and take mitigating acts accordingly, we also concur with this view and its reflection on contact tracing applications and believe that it would be beneficial to have such transparency in place for both data controllers and data subjects. Imagining that contact tracing applications with the possibility of reviewing the privacy conditions applied to them could be multiplying factor for the trust of data subjects in line with the GDPR and

⁷⁴⁸ Alrawais, Arwa; Alharbi, Fatemah; Almoteri, Moteeb; Altamimi, Beshayr; Alnafisah, Hessa and Aljumeiah, Nourah (2022) "Privacy-Preserving Techniques....", *op.cit.*, p.337.

⁷⁴⁹ *Ibid.*

⁷⁵⁰ Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines..." *op.cit.*, p.8.

⁷⁵¹ For the full Github documentation of Immuni see github.com/immuni-app/immuni-documentation.

⁷⁵² For the full Github documentation of eRouska see github.com/covid19cz/erouska-ios.

⁷⁵³ For the full Github documentation of Rakning C-19 see github.com/aranja/rakning-c19-app.

⁷⁵⁴ For the full Github documentation of CovTracer-EN see github.com/CovTracer-EN/covtracer-en-app.

⁷⁵⁵ For the full Github documentation of ProteGO Safe see github.com/ProteGO-safe.

⁷⁵⁶ For the full Github documentation of COVIDAlert see github.com/GOVMT-MITA.

⁷⁵⁷ Alrawais, Arwa; Alharbi, Fatemah; Almoteri, Moteeb; Altamimi, Beshayr; Alnafisah, Hessa and Aljumeiah, Nourah (2022) "Privacy-Preserving Techniques...", *op. cit.*, p.337.

ePrivacy transparency requirements, given that such applications utilize mobile technologies to quickly identify and inform users that may encounter with an infected person, thereby tackling the spread of Covid-19.⁷⁵⁸ In addition, these acts does not only increase the amount of preferences to download the application, but also solidify the perception of data subjects about their rights under the GDPR⁷⁵⁹ as well as the Charter of Fundamental Rights of The European Union.⁷⁶⁰

In conclusion, transparency requirement is of massive importance for indication of compliance with the GDPR requirements⁷⁶¹ by data controllers as set out in accountability and transparency articles. Having said that, some contact tracing applications employed within the EEA, particularly the ones we exemplified above, did put an effort to do that based on their privacy policies as well as terms and conditions of the use. However, such proactive approach with further solid enhancements should be implemented by all controllers across the Europe, considering the simplicity as well as the novelties in the implementation of transparency activities via different channels and means.

2.6 Data Subject Rights

Considering that in the digital age, the potential for data collection is huge⁷⁶², a pivotal part of the GDPR compliance activities of data controllers are consisting of the management of data subject rights. Moreover, when we consider the fact that was stated by Simón Castellano that one of the key

⁷⁵⁸ Simon; Trezn, Manuel.; Weiger, Welf H.; Tarafdar, Monideepa; Cheung, Christy M.K. (2020) "One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps", *European Journal of Information Systems*, vol.29, n.4, pp. 415-428, DOI: 10.1080/0960085X.2020.1784046, p.415.

⁷⁵⁹ Article 12 to 23 of the GDPR, data subject rights.

⁷⁶⁰ Article 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01), protection of personal data.

⁷⁶¹ Article 24 of the GDPR, responsibility of data controller.

⁷⁶² Blasi Casagran, Cristina, and Cañabate Pérez, Josep (2024) *Legislación y derecho digital para no juristas*, Servei de Publicacions de la Universitat Autònoma de Barcelona, (preview version available at Google Scholar), p.49.

challenges the Internet and the 2.0 world pose concerning reputation, privacy, and data protection is the boundless nature of digital memory⁷⁶³, we believe it is almost imperative for data controllers to act accordingly, and honour such data subject requests to mitigate these risks and open the door for data subjects' controller over their personal data. Hence, the GDPR aims to strengthen persons to have further control on their personal data and implementation thereof contains people, organizations and processes all together.⁷⁶⁴ Accordingly, to be more indicative, there are eight different data subject rights set out in the GDPR.⁷⁶⁵ These rights correspondingly include: the right to be informed, right to access, right to rectification (correction), right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object to processing, and right to not be subject to automated decision making, as detailed across article 12 to 23 of the GDPR. Therefore, in short, these rights provide individuals with further autonomy over their personal information and how they are used.

First of all, although in practice, implementation of data subject rights via both privacy-by-design and default methods and data subject requests attract a massive attention for both scholars due to the constant nature of processing activities, its room for contact tracing applications are not that much wide and complex due to the limited processing activities, as described in Chapter 1, 3 and 4. The fundamental reason is that as detailed in previous chapters almost each of the data controllers rely on unidentifiable data processing, and also in line with the storage limitation principle set out in Article 5 of the GDPR⁷⁶⁶,

⁷⁶³ Simón Castellano, Pere (2013) "A Test for Data Protection Rights Effectiveness: Charting the Future of the 'Right to Be Forgotten' Under European Law", *Columbia Journal of European Law Online*, pp.1-5, p.5.

⁷⁶⁴ Sideri, Maria, and Stefanos Gritzalis (2020) "Are we really informed on the rights GDPR guarantees?", In *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA, Mytilene, Lesbos, Greece, Proceedings*, n.14, pp. 315-326, Springer International Publishing, p.326.

⁷⁶⁵ Data subject rights referred in the articles are the right to be informed, The right of access, The right to rectification, The right to erasure, The right to restrict processing, The right to data portability, The right to object, Rights in relation to automated decision making and profiling.

⁷⁶⁶ See Article 5 of the GDPR, storage limitation.

they rely on limited storage period of processed data by default, i.e. 14 or 21 days, as detailed in Chapter 1. To be more specific, as clearly set out by Croatian application that pursuant to Article 11-2 of the GDPR, the Ministry is not required to collect additional data that make it possible for the previously mentioned information to be readily attributed to the user or mobile device user. It is neither necessary nor intended for the needs of the application.⁷⁶⁷ Given that this would require greater user information that is not currently available, it is not possible to directly enforce data privacy rights in line with Articles 15, 16, 17, 18, 20, and 21 of the GDPR.⁷⁶⁸ Similarly, the Irish app controller stated that in relation to the personal data that the app processed, data subjects have rights under the GDPR. Nevertheless, certain points regarding the processing of personal data by the application should be noted by data subjects before going on to list them.⁷⁶⁹ For instance, although IP addresses are utilized for temporary network routing and network security on the HSE servers, they are not stored there. Since diagnosis keys are intended to be non-identifying, they cannot be linked to an individual. Accordingly, the identities that are exchanged between phones and stored on phones via exposure notifications are not accessible to the data controller.⁷⁷⁰ Likewise, Estonian app also indicated that as there is not any personal data processing done by the app, it is not possible to exercise most of the rights set out under the GDPR,⁷⁷¹ and the Netherlands application indicated the same approach by reiterating that as CoronaMelder was created following the principles of data minimization and privacy by design, your ability to exercise your rights under the GDPR is somewhat restricted.⁷⁷² Therefore, as seen from these

⁷⁶⁷ Stop Covid Privacy Notice, *op.cit.*, section 11.

⁷⁶⁸ Stop Covid Privacy Notice, *op.cit.*, section 11.

⁷⁶⁹ HSE, privacy policy, *op.cit.*, section 12.

⁷⁷⁰ HSE, privacy policy, *op.cit.*, section 12.

⁷⁷¹ HOIA, privacy policy, *op.cit.*, section 14.

⁷⁷² Corona Melder, privacy policy, *op.cit.*, section 8.

concrete samples, data controllers right exclude the possibility of any identifiable data and data subject rights connection.

Having said that, there might be still room for illuminating some ambiguous aspects regarding data subject rights, considering that we did not witness loads of example of data subject requests, due to the nature of the processing activity, and there are potential “tricky” ways to reidentify data subjects as elaborated in Chapter 2. Nonetheless, instead of analyzing each of data subject rights separately, we will be focusing on the most remarkable and problematic aspects of data subject rights within the scope of the applications based on the technical features of the applications.

First, a significant challenge created by the applications is regarding the prioritization of data subject rights within the scope of contact tracing applications, as due to the technical and architectural design of the applications, it is not always feasible to exercise each of the rights set out in the GDPR. The fundamental reason is data protection does not take sole aim at information disclosure, in establishing a framework of rights and obligations aimed at achieving equitable balances among diverse societal objectives, fundamental rights, and personal freedoms, we contend that the manner in which privacy by design solutions weigh these rights against each other, while still posing substantial residual risks to data subjects, poses concerns.⁷⁷³ While recognizing the impossibility of attaining every ideal simultaneously, we advocate for transparent discussions on prioritizing certain rights and risks over others, emphasizing the need for accountable decision-making in this regard.⁷⁷⁴ For instance, well-known case, “Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja

⁷⁷³ Veale, Michael; Binns, Reuben and Ausloos, Jef (2018) "When data protection by design and data subject rights clash", *International Data Privacy Law*, vol.8, no. 2, pp. 105-123, p.121.

⁷⁷⁴ Veale, Michael; Binns, Reuben and Ausloos, Jef (2018) "When data protection by design ...", *op.cit.*, p.121.

González⁷⁷⁵, is scattered around right to be forgotten, due to the nature of the tool that process personal data, namely Google account of the data subject. Accordingly, as per this case law, data controller (Google) implemented the necessary actions resulted from decision accordingly, due to the closely connected nature of the request and processing activities itself, which did not prove it impossible to perform such request, considering the details of the case.

Likewise, the case related to Österreichische Post AG (the Austrian Postal Service) and had been referred to CJEU to address the scope of the right under Article 15(1)(c) of GDPR, the right to information on “the recipients or categories of recipient to whom the personal data have been or will be disclosed”, was requested by data subjects.⁷⁷⁶ Data controller, again, seemed to implement the necessary actions to complete the request, as per the details of the jurisprudence. Therefore, it is possible to state that although each data controller has a responsibility to facilitate the use of data subject rights set out under the GDPR, it would not be completely realistic to implement on the same level of each one due to the characteristic of the application and processing activity at stake, as some of them are comparatively more straightforward, whereas other requests could be particularly challenging for certain circumstances due to the nature of the processing activities. In this point, what we recommend is that by considering the risks linked to processing activities, as well as the technological features of the contact tracing applications, data controllers should be able to understand the most problematic and prone-to-abuse parts of processing activities of their own and

⁷⁷⁵ Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Request for a preliminary ruling from the Audiencia Nacional. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> (accessed on 5 April 2023).

⁷⁷⁶ For the full decision see the Judgment of The Court (First Chamber) 12 Jan 2023, RW v. Österreichische Post AG, REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings <https://curia.europa.eu/juris/document/document.jsf?jsessionid=3C5CC72DC7FD40E09826387758207064?text=&docid=269146&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=175897> (accessed on 5 April 2023).

prioritize data subject rights as per the vulnerability level of such type of right. In practice, it would end up increasing the quality of data subject rights. For instance, as briefly mentioned above, if the application claims not to process any identity data, how can data subjects exercise their right to data portability⁷⁷⁷ under the GDPR? Such requests are made to other organizations/entities processing massive amount of machine readable and portable personal data. Within the same remit, The Lithuanian data protection authority holds the opinion that data subjects ought to be capable of transferring to their payment account, including bank historical record and all payments made with their account, if they want to switch financial institutions,⁷⁷⁸ which is resulted from right to data portability, as the nature of the application from technical perspective, make such data subject request possible on the legal perspective as well. Or similarly, according to the Dutch supervisory authority and Slovenian supervisory authority, songs listened to through a service of streaming fall within the scope of the data portability right as well,⁷⁷⁹ in which case, we are of the view that, changing from one data controller to another is possible, whereas such an option is not really viable for contact tracing applications.

To be more precise, it might be possible to transfer the processed unidentified data to other European contact tracing applications performing under common European framework⁷⁸⁰, Gateway, which will be detailed in Chapter 5 under Interoperability discussions. In other words, considering that data transfer is possible within the scope of interoperability matter, technically there

⁷⁷⁷ See Article 20 of the GDPR, right to data portability.

⁷⁷⁸ Reus, Jurre and Bilderbeek, Nicole (2022) "Data Portability in the EU an Obscure: Data Subject Right", IAPP <https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/> (accessed on 23 June 2024).

⁷⁷⁹ Reus, Jurre and Bilderbeek, Nicole (2022) "Data Portability in the EU an Obscure: Data Subject Right", IAPP <https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/> (accessed on 23 June 2024).

⁷⁸⁰ See European Commission Website Press Release, Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043 (accessed on 11 April 2023).

is a chance to implement such portability of personal data, with a different and adjusted approach than classical means of portability at the first glance. However, it is important to distinguish between the term of data controller. In the case of interoperability matters, all of the data controllers deemed as “joint controller”⁷⁸¹, whereas as seen from the various samples provided herein, data portability is possible, when there are different data controllers at stake. Therefore, due to the design of the processing activities, it is not realistic to assume that this right is feasible in the contact tracing regime. Similarly, considering that there is not any automated decision-making system involved in digital contact tracing process, data subjects could not be able to exercise their right under Article 22 of the GDPR⁷⁸² either.

Hence, investing on the right direction of data subject requests would solidify contact tracing applications’ ability to respond such requests in a quickest way. Considering that data subject requests require a lot of sources to invest on, it would not really be a wise decision to invest in each type of data subject rights, regardless of the other factors delineated above. Accordingly, we would like to pinpoint the most challenging and charming aspect of data subject requests, which are namely right of access⁷⁸³ and right to erasure⁷⁸⁴, due to the nature and ambiguity of processing methodology, on which data controllers keep investing the right amount of effort and monetary sources. Having said that, we believe that analysis of the exceptions to the requirement provided by the EDPB would be adjusted to this case scenario as well, in which it provided interpretation of the GDPR based on the CJEU case law that

⁷⁸¹ See European Commission, National Joint Controllers and privacy policies of contact tracing applications available at https://health.ec.europa.eu/system/files/2023-02/gateway_jointcontrollers_en.pdf (accessed on 23 June 2024).

⁷⁸² Article 22 of the GDPR, automated individual decision making.

⁷⁸³ Article 15 of the GDPR, right of access of data subject.

⁷⁸⁴ Article 17 of the GDPR, right to erasure.

was rendered,⁷⁸⁵ to provide data controllers with the right amount of time to allocate for the highly prioritized bunch of data subject request. To be more specific, given that it creates loads of workload on data controllers, from the efficiency point of view, delivering the most efficient outcome, it is unrealistic to assume that data controllers would mitigate the concerns delineated in Chapter 2 by only exercising data subject access or deletion requests. To this end, the GDPR sets out the right of access is without any general reservation to proportionality about the efforts the controller must take to comply with the data subject's request.⁷⁸⁶ Particularly, this derogation is creating a standpoint for the controllers of the applications as well. Based on the privacy policies detailed in Chapter 1, most of the applications either not process personal data for longer than maximum three weeks, or not process personally identifiable data. Therefore, under this derogation, it would obviously cause disproportionate effort to retrieve the personal data processed. In addition, even if it was possible to retrieve the deleted personal data after 2 or 3 weeks, it would be implicitly accepting the fact that this personal data could be retained beyond the expectations of data subjects, which would solidify the fears and concerns raised in Chapter 2.

Furthermore, with regards to the second type of exception set out in the GDPR, there could be, theoretically, another valid exception that could apply to the controllers, namely adversely affecting the rights and freedoms of other data subjects⁷⁸⁷, also considering that the EDPB is supportive of the idea that The controller has to be able to display how the situation would adversely affect the rights or freedoms of others.⁷⁸⁸ We believe that due to the aforementioned reasons, rights of other data subjects are not likely to be impacted by such an act, therefore it is not applicable to contact tracing

⁷⁸⁵ EDPB (2023) Guidelines 01/2022 on data subject rights- Right of access, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (accessed on 23 June 2024), p.9.

⁷⁸⁶ EDPB (2023) Guidelines 01/2022 on data subject rights - Right of access, p.4.

⁷⁸⁷ Recital 63 of the GDPR, Right of Access.

⁷⁸⁸ EDPB (2023) Guidelines 01/2022 on data subject rights - Right of access, p.4.

context. On the other hand, it might be deemed disproportionate as stated by the EDPB⁷⁸⁹, and even abusive sometimes, depending on the context, as this occasion of processing within scope of contact tracing activities must be treated differently than other “Business as usual⁷⁹⁰” processing activities.

That said, based on our review of existing contact tracing applications’ privacy and website policies, as a promising sign of compliance with the right to be informed⁷⁹¹, they were notified with regards to use of their rights, which, we believe, as detailed in related section of this Chapter, creates the most fundamental aspect of data subject rights. Considering the nature of the processing activities of the apps, bundling the description and the fate of all data subject rights in a single source of information with coherent approach, is therefore more in line with the reality. For instance, Cyprus, Estonia, French, German, Slovenia, Belgium and Czech applications are some samples of this approach.⁷⁹² This is also important for data subjects to create any ambiguity regarding to whom they are going to exercise their right towards, as detailed in transparency and accountability section, as, it is clear that the performance of these rights could pose significant difficulties due to the practicalities involved in knowing each controller that is processing the personal data at stake.⁷⁹³ Hence, as said, it is feasible to strengthen the capabilities of data controllers predominantly for exercisable rights, such as right to access and

⁷⁸⁹ EDPB (2023) Guidelines 01/2022 on data subject rights - Right of access, p.4.

⁷⁹⁰ As per the Indeed Article, Business as usual refers broadly to any situation where everything is proceeding as normal and as expected. In a business context, a BAU process is any element of day-to-day operations that are largely the same day after day. Available at: <https://www.indeed.com/hire/c/info/business-as-usual> (accessed on 12 April 2023).

⁷⁹¹ See article 13 of the GDPR, Information to be provided where personal data are collected from the data subject.

⁷⁹² See Tous Anti Covid app, privacy policy, *op.cit.*, section “exercising your rights”, eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, *op.cit.*, section “your rights”, OstaniZdrav privacy policy, *op.cit.*, section 13, Coronaalert privacy policy, *op.cit.*,10, Corona Warn, privacy notice, *op.cit.*, section 13, CovTracer-EN, Privacy policy, *op.cit.*, section 12.

⁷⁹³ Politou, Eugenia; Michota, Alexandra; Alepis, Efthimios; Pocs, Matthias and Patsakis, Constantinos (2018) "Backups and the right to be forgotten in the GDPR: An uneasy relationship", *Computer Law & Security Review* 34, no. 6 pp.1247-1257, p.1250.

right to deletion, and keep supporting such act with detailed and easy-to-digest type of notice. Accordingly, some of the rights should be prioritized according to the nature of processing, given that non-existence of personal data processing and implementation of all data subject rights are bit incoherent for some controllers. Based on our review of the policies, not all controllers prioritized any data subject rights over the other one, except for the countries mentioned above.

On the contrary, it is seen that some of them elaborated each of data subject rights either, which we believe that important multiplier of the ambiguity delineated in this chapter, as it potentially gives the impression that all rights are exercisable because personal data processing took place. Particularly, the most detailed approach was indicated by the Austrian, Lithuanian, Denmark and Poland applications.⁷⁹⁴ Although it is good to have such detailed approach, due to the aforementioned reasons, it might create confusion and ambiguity about non-existence of personal data, therefore, we are of view that aforementioned approaches brought by other controllers are more consistent with the idea of processing non-identifiable data. For instance, revisiting the right to be forgotten portion of the rights, which is described by Miquel Peguera, as a broad concept that pertains to individuals' ability to control the spread and ongoing availability of information about themselves⁷⁹⁵, how can data controllers who claim they do not process any identifiable data fulfill such a broad request? Similarly, we also understand that such ambiguity is also felt in the controllers' end, due to the unexpected and quick nature of the pandemic, and potentially the logic how they would like to build a logic in line with the GDPR requirements. As such, in consideration of such potential confusions, we believe that going forward, controllers should provide more

⁷⁹⁴ See the Stop Corona App. Privacy policy, *op.cit.* section 7; Smittestop privacy policy, *op.cit.* section 8, Karantinas privacy policy, *op.cit.* section 12, ProteGO Safe privacy policy, *op.cit.* section "Users' rights".

⁷⁹⁵ Peguera Poch, Miquel (2019) "The right to be forgotten in the European Union", *The Oxford Handbook of Online Intermediary Liability (OUP, 2019 Forthcoming)*, pp.1-16, p.16.

clear and coherent explanation on available rights of data subjects, in light of the non-personal data processing activities aimed by controllers.

Subsequently, another challenge on exercising data subject requests, thereby rights, is related to the verification of the identity of data subjects, as mandated by the GDPR with regards to the exercise of data subject requests.⁷⁹⁶ Typically, if the data controller has uncertainties about the identity of the individual making a request, they may demand additional information as evidence.⁷⁹⁷ Specifically, when information is sought verbally, the data controller must possess proof of the requester's identity before disclosing any information.⁷⁹⁸ However, odd enough, as reiterated above, technical feature of most contact tracing applications do not allow the verification of the identity, which is expected the privacy-friendly approach though. Nevertheless, it would be creating a real challenge for the implementation of data subject rights in general based on recital 64 of the GDPR. Notwithstanding this challenge, we are of the view that data subject rights could still be implemented in a way that is specific to the contact tracing applications. To be more concrete, other identity verification methodologies could be utilized to implement such data subject requests, such as using the unique codes generated by the applications for the installation or any other unique identifiers that could not reveal the identity of the user but rather only act as a numerical identifier. By such method, both risks delineated in Chapter 2 could be prevented and at the same time utilization of data subject rights could safely conducted by data controllers, in line with the spirit of the GDPR. This verification is important for the prevention of any potential data breach and abuse of personal data. Most security professionals concur that employee

⁷⁹⁶ Recital 64 of the GDPR, verification of data subject.

⁷⁹⁷ True Vault Website Article, What Are the Rights of Data Subjects Under GDPR <https://www.truevault.com/resources/compliance/what-are-the-rights-of-data-subjects-under-gdpr> (accessed on 12 April 2023).

⁷⁹⁸ True Vault Website Article, What Are the Rights of Data Subjects Under GDPR <https://www.truevault.com/resources/compliance/what-are-the-rights-of-data-subjects-under-gdpr> (accessed on 12 April 2023).

mistakes are the main cause of data leaks within the company.⁷⁹⁹ When there are human agents present, they may be coerced or socially engineered into disclosing information.⁸⁰⁰ In addition to the risks delineated in Chapter 2, for this case scenario, it is important to be aware of this sort of abuses as well. Therefore, due to the augmented risk resulting from processing unidentifiable data of data subjects, or complete deletion after 2-3 weeks, it is often almost impossible to verify the identity of the data subject, which automatically proves challenge for controllers to address by implementing cutting edge technical methodologies.

Finally, the issue of notifying external processors regarding the exercise of data subject requests, in particular deletion requests within the scope of right to erasure under the GDPR, is most vulnerable to such ambiguity due to the structure of the applications. Pursuant to article 19 of the GDPR, in accordance with Article 16, Article 17(1), and Article 18, the controller shall notify each recipient to whom the personal data was previously disclosed of any correction, erasure, or restriction of processing that has been made, unless doing so proves to be impractical or requires disproportionate effort.⁸⁰¹ Particularly, considering that the right to erasure is the most related and potential request among other rights and the third party involvement is quite a common component of the applications as explained previously, any change in the situation of the processed data, even if within the limited period time of the storage, must be reflected on to third parties as well. As per the GDPR, in case data controller disclosed data at stake to any third parties, controllers must notify the third party regarding the erasure or restriction of the

⁷⁹⁹ Protecto Website Article, Common Problems in Handling Data Subject Access Requests <https://www.protecto.ai/blog/common-problems-in-handling-data-subject-access-requests-dsars> (accessed on 12 June 2024).

⁸⁰⁰ Protecto Website Article, Common Problems in Handling Data Subject Access Requests <https://www.protecto.ai/blog/common-problems-in-handling-data-subject-access-requests-dsars> (accessed on 12 June 2024).

⁸⁰¹ See Article 19 of the GDPR, Notification obligation regarding rectification or erasure of personal data or restriction of processing.

personal data.⁸⁰² As such, the third parties will also be obliged to erase or restrict the personal data they retain.⁸⁰³ Based on the EU data and the information provided by them, vast majority of the applications utilized third parties for the development or implementation of their apps, such as Czech app using Seznam.cz, PaleFire Capital, O2, and the other private companies, whereas Slovenian app used RSTEAM company, or Spanish app used Indra Sistemas SA company for the development of the app, and Iceland app used Stokkur, Aranja, Samsýn, Kolibri, Sensa companies.⁸⁰⁴ Hence, we believe that most of the controllers must have covered this aspect in their contracts and such contracts would also solidify this mechanism.

Nevertheless, the issue has further complications due to both nature of data processed and statements of third-party service providers concerning not accessing any data processed within the scope of the contact tracing activities, as detailed in Chapter 1. In other words, even when controllers do have knowledge of the third parties processing some data that they collected, it places upon them the additional obligation to inform those third parties about the erasure request.⁸⁰⁵ Furthermore, taking into account that the personal data was already backed-up or archived by the controller or by the third parties, and then the challenge for implementing this requirement looks also indisputable.⁸⁰⁶ Accordingly, we believe that data controllers must be mindful about the definitions of data subject rights at stake, to keep their consistency

⁸⁰² ICO, “The right to erasure and the right to restriction” <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/the-right-to-erase-and-the-right-to-restriction/> (accessed on 12 April 2023).

⁸⁰³ ICO, “The right to erasure and the right to restriction” <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/individual-rights/the-right-to-erase-and-the-right-to-restriction/> (accessed on 12 April 2023).

⁸⁰⁴ For the full details on the third-party companies taking place in the develop see European Commission Digital Contact Tracing Study on lessons learned (2022), op.cit., Annex II, Country Research, p.120-p.190.

⁸⁰⁵ Politou, Eugenia; Michota, Alexandra; Alepis, Efthimios; Pocs, Matthias and Patsakis, Constantinos (2018) “Backups and the right to be forgotten in the GDPR...”, op.cit., p.1250.

⁸⁰⁶ Politou, Eugenia; Michota, Alexandra; Alepis, Efthimios; Pocs, Matthias and Patsakis, Constantinos (2018) “Backups and the right to be forgotten in the GDPR...”, op.cit., p.1250

regarding their data protection compliance activities. Having said that, another component of this aspect of third party and data subject request is related to handling of request via third party intermediaries. For organisations, these portals could be seen as providing an easier way of dealing with rights requests in one place.⁸⁰⁷ Providing perhaps, a more secure way of sharing personal data, for example in responding to a data subject access requests set out in the GDPR⁸⁰⁸. In such circumstances that data controllers opt for using external third party to handle data subject requests, they must be mindful about the disclosure of personal data or any other identifiable data to third parties, and its onward distribution. Correspondingly, controllers must establish a methodology that does not allow any of these concerns to occur and to allow any third parties to identify application users. This is lying in the trust sense of third-party data processors, and efficient safeguards envisaged for such third-party engagements. As detailed in security of processing part of Chapter 4, implementing a detailed due diligence for the selection of third parties which are going to handle data subject requests are one of the keys of the successful compliance with this portion of the legislation⁸⁰⁹. Moreover, within the same remit, the contractual mechanism is also important contributor to this part, given that any third-party processor involved in processing activity will be obliged by the articles of the contract to implement such deleting requests without any delay, and in line with the direction provided by controllers of the applications, whose details shared in security of processing part of Chapter 4.

To conclude, we are of the view that need for implementation of data subject rights are kept limited considering the explanations in this section. The fundamental reason is that the GDPR allows a data subject to more easily exercise his rights if there is a clear indication that his data are not adequately

⁸⁰⁷ DP Network Website, Managing Erasure Requests or DSARS via Third Party Portals (<https://dpnetwork.org.uk/managing-erasure-requests-dsars-third-party-portals/> accessed on 12 April 2023).

⁸⁰⁸ See Article 15 of the GDPR, right of access by data subject.

⁸⁰⁹ See Article 17 of the GDPR, right to erasure.

protected.⁸¹⁰ Having said that, the rights of the data subject, however, do not really allow them to proactively and substantially assert control over the processing of his personal data.⁸¹¹ Thus, theoretically, data subjects have plenty of rights, and also have a range of sources to be informed on their rights.⁸¹² Nonetheless, given that some data subjects may not be able to find this information or discard it exists, information campaigns implemented on national basis and mass media sourced information are quite significant,⁸¹³ which was detailed in transparency and accountability section of this Chapter. Correspondingly, the goal of data controllers is to create a processing relationship which does not oblige data subjects to need to use their rights at all, and to meticulously inform them about every single right protected by them. As a natural outcome of such situation, there are not loads of instances nor discussion pertaining to exercise of data subject rights as part of the use of the applications within the EEA/EU. In line with this idea, data subjects feel less obliged to exercise their rights against controllers, due the guarantee provided by data controllers with regards to not processing any identifiable data that could be required to implementation of data subject rights. Although almost each of the controllers mentioned the existence of a chance to implement data subject rights in their documentation on some level, some more detailed, whereas others less, or some more coherent, while others were more ambiguous, as discussed above. Therefore, we believe that going forward, recommendations provided in this section should be applied to data subjects, through which data subjects would feel less and less obliged to exercise their rights, as the most optimal privacy and data protection conditions are going to be provided to them by default without any ambiguity.

⁸¹⁰ Wolters, P. T. J. (2018) "The control by and rights of the data subject under the GDPR.", p.16.

⁸¹¹ Wolters, P. T. J. (2018) "The control by and rights of the data subject under the GDPR.", p.16.

⁸¹² Sideri, Maria, and Stefanos Gritzalis. "Are we really informed on the rights GDPR guarantees?" In *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings, 14*, pp. 315-326. Springer International Publishing, p. 325.

⁸¹³ Sideri, Maria, and Stefanos Gritzalis. "Are we really informed...", op.cit., p. 325.

IV- CONTROLLER/PROCESSOR OBLIGATIONS UNDER THE GDPR

1. Processing of Location data

Pursuant to Recital 78⁸¹⁴ of the GDPR, the controller ought to create internal policies and establish protocols that explicitly align with the principles of data protection by design and default, ensuring they demonstrate adherence to this Regulation and compliance with its requirements. Such steps could include, among other things, limiting the processing, pseudonymizing personal data as quickly as possible, being transparent about the purposes and methods of processing, allowing the data subject to keep an eye on the data processing, and allowing the controller to develop and enhance security features. The same logic applies to the processing of location data of the data subjects within the scope of contact tracing activities in Europe. Accordingly, data controllers are also required to mitigate the risks elaborated in Chapter 2 under Location Data, Data Management and Architecture of the Applications sections in their processing activities. Either pseudonymising or anonymized data processing within the scope of location data collection is of beneficial to the data controllers to comply with the GDPR.

As delineated in Chapter 1, contact tracing applications process sensitive personal data i.e. phone numbers, MAC addresses as well as GPS location data.⁸¹⁵ In other words, location data can be gathered in several ways, each

⁸¹⁴ Recital 78 of the GDPR indicates that safeguarding the rights and freedoms of individuals regarding personal data processing necessitates employing suitable technical and organizational measures to uphold the requirements of this Regulation. To exhibit compliance, the controller must adopt internal policies and implement measures that specifically align with the principles of data protection by design and default. Such measures may include minimizing personal data processing, promptly pseudonymizing personal data, ensuring transparency about data functions and processing, enabling data subjects to oversee data processing, and empowering controllers to establish and enhance security protocols. In the creation, design, selection, and utilization of applications, services, and products reliant on personal data processing, creators of these offerings should be encouraged to prioritize data protection rights. They should, considering technological advancements, ensure that controllers and processors can fulfil their data protection duties.

⁸¹⁵ Alshawi, Amany; Al-Razgan, Muna.; AlKallas, Fatima H; Bin Suhaim, Raghad Abdullah; Al-Tamimi, Reem; Alharbi, Norah and AlSaif, Sarah Omar. (2022) "Data privacy during pandemics: a systematic literature review of COVID-19 smartphone applications", PeerJ Computer Science, vol. 7, pp.1-29, p.8.

with varying degrees of accuracy (for example, via Wi-Fi access points, GPS, cellular carriers, location suppliers, or location! aggregators).⁸¹⁶ To be more concrete with the definitions, even though location data does not fall under the GDPR definition of special categories of data, it does concern potentially sensitive and intrusive information with regards to the private life of the data subjects. Consequently, according to this approach, the European ePrivacy Directive clearly stipulates that the processing of precise location data for value-added services is only allowed if users have provided their consent.⁸¹⁷

First, we believe that two-fold approach would be a useful starting point to remediate such potential problems linked to location data. To be more specific, this might be converted into appropriate tools for data subjects to regulate the usage of their data, combined with privacy appropriate settings.⁸¹⁸

The problem of location data highlights the distinction between settings that govern access to personal data and settings that govern how the data is utilised. As a first step, suitable settings may allow the data subject to control whether his/her location data is shared, in line with opt-in mechanism detailed in Chapter 4. Second, these settings will allow the data subject to control how their personal data is utilised. In some cases, the end-user may not be able to control access to their location data, and the position of a device can be inferred via its Wi-Fi access point or from its local cache files.⁸¹⁹ Digital contact tracing application contact logs should adhere to the principles of privacy by design and data minimization by collecting only an anonymized identifier unique to each contact utilized.⁸²⁰ This means the applications should not

⁸¹⁶ Ausloos, Jef; Kindt, Els; Lievens, Eva; Valcke, Peggy and Dumortier, Jos (2013), "Guidelines for privacy-friendly default settings", *ICRI Research Paper*, n.12, available at SSRN: <https://ssrn.com/abstract=2220454> or <http://dx.doi.org/10.2139/ssrn.2220454>, pp.1-34, p.9.

⁸¹⁷ Ausloos, Jef; Kindt, Els; Lievens, Eva; Valcke, Peggy and Dumortier, Jos (2013) "Guidelines for privacy-friendly...", *op.cit.*, p.10.

⁸¹⁸ Ausloos, Jef; Kindt, Els; Lievens, Eva; Valcke, Peggy and Dumortier, Jos (2013) "Guidelines for privacy-friendly...", *op.cit.*, p.10.

⁸¹⁹ Ausloos, Jef; Kindt, Els; Lievens, Eva; Valcke, Peggy and Dumortier, Jos (2013) "Guidelines for privacy-friendly...", *op.cit.*, p.9.

⁸²⁰ O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; et al. (2021) "Best practice guidance for digital contact tracing...", *op.cit.* p.8.

record the name, age, sex, ethnicity, or address of the contact nor should it record the time or location of the contact event.⁸²¹ Nevertheless, by using such opt-in mechanism, data subjects would be granted to more flexibility to determine as to which location related data they would be willing to provide for contact tracing activities. This is, evidently, the floor basis of efficient implementation of strict location data processing, and it is not realistic assume that employing a straightforward opt-in mechanism would mitigate all of the concerns detailed in Chapter 2.

Therefore, in line with this logic, rather than simply pointing out the opt-in mechanism, more realistically, the EDPB pointed out that anonymized data processing should always take precedence over personal data processing⁸²², as elaborated in the next section. In this respect, such processing entails considering entire location datasets as well as processing data from numerous people utilizing existing strong anonymization techniques, if they are properly and successfully applied. The only data relating to the users is their mobile phone number, which is held on a secure server managed by the health authorities, as detailed by many countries' controllers in their privacy policies, i.e. Denmark⁸²³ and these apps did not use the user location data or other identifiable data, therefore, contact of affected people would never be able to identify the person testing positive for the virus, as stated in most applications policies, such as or Germany⁸²⁴, or Slovenia⁸²⁵. Similarly, the first edition of Poland's ProteGO Safe app employed Bluetooth technology to monitor connections between smartphones on a device.⁸²⁶ An infected user

⁸²¹ O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; et al. (2021) "Best practice guidance for digital contact tracing...", *op.cit.* p.8.

⁸²² EDPB (2020) Guidelines 04/2020, *op.cit.*, p.5.

⁸²³ See Smittestop, Privacy Policy, *op.cit.* section "for what purpose can my data be used?"

⁸²⁴ See Corona Warn, Privacy notice, *op.cit.* section "access data" and section "exposure data".

⁸²⁵ See OstaniZdrav, Privacy Notice, *op.cit.*, section 7.

⁸²⁶ See Reuters, (2020) Poland rolls-out privacy secure coronavirus tracking app <https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN23G208> (accessed on 23 June 2024).

would modify his status in the application anonymously, and the program would communicate data about his contacts in the preceding two weeks to an external server to alert other users about the potential risk. However, concerns over privacy and security led Poland to join Latvia, and Italy in using Bluetooth short-range radio for their apps, which is based on Apple AAPL.O and Google GOOGL.O technology that securely logs exchanges on the cell phones of persons who have been in proximity.⁸²⁷

Accordingly, in light of these problematic aspects of controllers, we also agree with the common view that proximity-based approach has inherent advantage over the geolocation data from the GDPR lens, considering that its sensing could be implemented in a manner that is privacy-sensitive without loads of effort. For example, Li and Guo supports the idea that arguably the decentralized and no GPS solution brings the highest level of data protection for individuals as not any personal data is processed unless the user is infected.⁸²⁸ Without having the GPS tracking, applications cannot collect and trace the movement of the population on geographical basis. With a decentralised framework, yet any data collected from individuals cannot be driven into a centralized database for future analysis, i.e. limited amount of information could be supplied to governments for monitoring the self-quarantine and the advancement of the disease in society.⁸²⁹

Therefore, we are of view that with this approach, absolute location-related information is neither collected nor shared. Variants of proximity-based analyses have been employed in the past for privacy-sensitive analyses in healthcare.⁸³⁰ Taking advantage of proximity-based signals could accelerate

⁸²⁷ See Reuters, (2020) Poland rolls-out privacy secure coronavirus tracking app <https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN23G208> (accessed on 23 June 2024).

⁸²⁸ Li, Jinfeng, and Guo, Xinyi (2020) "Global deployment mappings and challenges of contact-tracing apps for COVID-19", *Available at SSRN 3609516*, pp.1-7, p.4.

⁸²⁹ *Ibid.*

⁸³⁰ Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols...", *op.cit.*, p.3.

the process of contact discovery and enable contact tracing of people that is otherwise difficult to discover, which is exactly what the GDPR and the ePrivacy Directive desire to see in data controllers' practices. This method can also be implemented without third-party involvement, offering similar privacy trade-offs to manual contact tracing.⁸³¹ Moreover, this functionality can allow someone that has illness with symptoms which is consistent with Covid-19, or who tested positive for Covid-19, thereby confirming their infection, to share information that may be in relation to the wellness of other people, on a volunteer basis and under pseudonymization.⁸³²

Nevertheless, it is important to note that, as detailed in the previous sections, the Norwegian application Smittestop was imposed a ban as stated by the Data Protection Authority Director-General, as they concluded that the utilization of location data for digital contact tracing proved to be unnecessary, thus, they recommend the use of Bluetooth data only. Also, they added that they did not find that the data controller of the app could sufficiently justify the need to use location data for contact tracing and await new information from the data controller.⁸³³ In light of this sample, it is plausible to state from the compliance perspective that certain legal justifications under the GDPR⁸³⁴ is strictly required for the any sort of location processing activities of the applications. This justification must also be in line with the necessities of data minimization practices detailed in this chapter. However, to take a step further from what is discussed in the relevant literature, we need to understand whether proximity-based approach is useful to minimize the risks associated with location data. In other words, although as said, proximity-based

⁸³¹ Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols and mechanisms....", op.cit., p.3.

⁸³² Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols and mechanisms....", op.cit., p.3.

⁸³³ For the full decision see EDPB, Temporary suspension of the Norwegian Covid-19 contact tracing app https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en (accessed on 23 August 2022).

⁸³⁴ See Article 6 of the GDPR, lawfulness of processing.

(Bluetooth) has an inherent advantage over the location data, it should still not be deemed as an error-free approach.

The reason is that as mentioned in the data minimization section, with the help of cutting-edge technologies, it is still possible to abuse data minimization practices. It is obviously damaging to the legal compliance of data controllers, under the coverage of advanced technical methodologies. Therefore, rather than strictly coming up with a solution that Bluetooth is risk-free for data location, it is more important to promote a system that can manage, in a privacy-sensitive style, data regarding people that came in close proximity to them over a period of time (e.g., the last two weeks), even if there is not any personal connection among these individuals.⁸³⁵ Additionally, since access to user health data and location data, both are needed for the correct functioning of the system, it becomes genuinely crucial that the system specifications, design, and development be considered as inter-disciplinary user-focus research taking into account the social, and psychological, security and human-computer interaction aspects of users while designing solutions satisfying the needs of the healthcare workers.⁸³⁶ In particular, considering that there are many advanced tracing activities happening these days by relying on a significant amount of location-related data of data subjects. A prominent example of a technologically advanced means of location tracking is the decision of the Dutch Data Protection Authority on the municipality of Enschede which decided to measure how crowded the city centre was, using sensors by a help of contracted a company that specializes in conducting people counts.⁸³⁷ A local government and two companies were able to access the data. Also, as Verdier explains on the EDPB website, "the use of Wi-Fi

⁸³⁵ Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi (2020) "Pact: Privacy sensitive protocols and mechanisms....", op.cit., p.3.

⁸³⁶ Trivedi, Ameer and Vasisht, Deepak (2020) "Digital contact tracing: technologies, shortcomings, and the path forward", *ACM SIGCOMM Computer Communication Review*, vol.50, no. 4, pp.75-81, p.80.

⁸³⁷ For the full description and decision see European Commission Website, Dutch DPA fines municipality for Wi-Fi tracking.

https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en (accessed on 23 June 2024).

tracking is subject to strict conditions and is banned in most cases. This technology has a significant impact on people's daily lives. It should only be used in exceptional cases, because in some circumstances local governments are permitted to use Wi-Fi tracking to process personal data, for example, to comply with statutory obligations. if you must fulfil it. That said, they added that if the DPA establishes that a municipality or business is using Wi-Fi tracking unlawfully, they run the risk of a hefty fine.⁸³⁸

Our view is on the utilization of this concrete sample for contact tracing apps that although nature of the processing activity differs from the contact tracing, the tracing activity in a different manner posed a risk on individuals as per the tracking technology utilized within this incident, as detailed above. As a key take away, considering the numerous newly emerging technologies for tracking, as in line with this sample regarding Wi-Fi tracking, it is important to employ most up-to-date and cutting-edge solutions as for the security of processing location data as set forth under the GDPR⁸³⁹ as well. Within this respect, from our perspective, using blockchain technology could be one way to achieve this requirement. Blockchain is a distributed ledger that stores everyone's data in an accessible, auditable, and tamper-proof decentralized storage solution, addressing trust and transparency issues while also protecting user privacy and accessibility.⁸⁴⁰ Hence, Blockchain is a chain-like data structure composed of blocks with a header and a body that are linked together using a hash tree.⁸⁴¹ Each block has a header with a hash value associated with the previous block's content, forming a retroactive link from

⁸³⁸ For the full description and decision see European Commission Website, Dutch DPA fines municipality for Wi-Fi tracking https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en (accessed on 23 June 2024).

⁸³⁹ Article 32 of the GDPR, security of processing.

⁸⁴⁰ Klaine, Paulo Valente, Zhang, Lei; Zhou, Bingpeng; Su, Yao; Xu, Hao and Imran, Muhammad (2020) "Privacy preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic", *IEEE Internet of Things Magazine*, vol.3, n.3, pp. 58-63, p.60.

⁸⁴¹ *Ibid.*

the most recent block to the genesis block, the chain's first block.⁸⁴² It offers an unbreakable link to the fully traceable records in the sequence of blocks; as a result, users can ensure the validity and authenticity of any known block by determining the hash code and comparing it to the next block.⁸⁴³ As a result, every network participant keeps a copy of the data, to find the most recent block on the longest chain, it is what makes the network decentralized.

Indeed, this should only apply to situations and implementations in which data is being processed and/or stored in a form that allows for such rectification and where the above-mentioned negative impacts are likely to occur. It is stressed by the data controllers of contact tracing applications, there was no location data or any other data that identifies location was collected, except the anonymous exposures with the contact. From this standpoint, it is beneficial for the privacy of the society that contact tracing can alert people only when they encounter with a person that might be subject to risk. In some countries, such as Italy for example, technology experts did not rule out a priori the possibility of collecting limited amounts of geolocation data for decentralized contact tracing purposes, but this option never gained support in policy circles.⁸⁴⁴ The rationale, based on data protection by design, is that geolocation data is considered redundant to the aim of proximity tracing, since it contains more information than is necessary to notify users about contact with positive cases.⁸⁴⁵ However, this argument depends upon a specific view of digital contact tracing as a personal warning system, which we find quite useful to enlighten the unclear perception about location data is “bad”, and Bluetooth is “good” sort of approach. From our perspective, Google Apple solution is also offering a secure and privacy friendly approach from the location data perspective, although it is still subject to some criticism, which

⁸⁴² Klaine, Paulo Valente, Zhang, Lei; Zhou, Bingpeng; Su, Yao; Xu, Hao and Imran, Muhammad (2020) "Privacy preserving contact tracing... ", *op.cit.* p.60.

⁸⁴³ *Ibid.*

⁸⁴⁴ Blasimme, Alessandro; Ferretti, Agata and Vayena, Effy (2021) "Digital contact tracing against COVID-19...", *op.cit.*, p.7.

⁸⁴⁵ *Ibid.*

will be detailed in the following chapters. The Apple/Google framework, as is well known, suggests a decentralized data structure to protect privacy and halt governments from discovering a network of social contacts⁸⁴⁶, and almost any phone broadcasts a separate identifier that was generated by rolling cryptography. The Google/Apple Exposure Notification (GAEN) system also relies on BLE RSS-based distance measurements between devices and a decentralized architecture like DP-3T. Not any location information is stored regarding the users' keys and stores identifiers broadcasted from devices in the surrounding.⁸⁴⁷ Furthermore, as detailed in the privacy-by-design section in Chapter 4, the GAEN system is relying on the differential privacy method, which was developed by Google and Apple in collaboration with public health authorities.⁸⁴⁸ Differential privacy is a mathematical method for adding randomness to a dataset to protect any person from attaining information regarding individuals in the relevant dataset.⁸⁴⁹ From the GDPR perspective, differential privacy offers a cutting-edge and smart solution for obscuring the location of the data subjects in a secure and open way. The system uses Bluetooth signals to determine whether users have been near each other, but it does not reveal the identities or locations of the users. The GAEN system, accordingly, uses differential privacy to add random noise to the Bluetooth signals, further protecting user privacy. In that aspect, the system has been praised for its location protection feature, and we also believe that by adding random noise to the data collected by the app, it can protect the privacy of individuals while still allowing for useful data analysis and would offer a

⁸⁴⁶ Kleinman, Robert A., and Merkel, Colin (2020) "Digital contact tracing for COVID-19", *Cmaj*, vol.192, no. 24 pp. E653-E656, p.E654.

⁸⁴⁷ Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2020) "October. Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control. In 2020 12th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)", pp. 229-235, p.233.

⁸⁴⁸ Apple Website, Contact Tracing <https://www.apple.com/covid19/contacttracing> (accessed on 21 August 2022).

⁸⁴⁹ Dilmegani, Cem (2024) "Differential Privacy: How It Works, Benefits & Use Cases in 2024", AI Multiple Research, <https://research.aimultiple.com/differential-privacy/> (accessed on 23 June 2024).

solution in line with what we proposed for both geolocation and Bluetooth solution from the legal perspective.

Correspondingly, as a further input for the GPS location tracking discussion, in order to understand the limits of the boundaries of localization utilization for data controllers of these applications, guidance prepared by the European Court of Human Rights⁸⁵⁰ ('the ECHR') and geolocation related part thereof⁸⁵¹, the guidance mentioned *Uzun v. Germany*, 2010, §§ 51-52⁸⁵² case as a sample to discuss whether GPS devices constitute personal data, as they may reveal a person's whereabouts and public movements, and the processing and use of this data may be viewed as a violation of the data subject's right to respect for their private life. According to the Court Decision, the surveillance via GPS, conducted in the context of the case, was deemed proportionate to the legitimate objectives pursued, thereby considered "necessary in a democratic society" as outlined in Article 8 § 2.⁸⁵³

However, at the same time, in another case where the Court examined the question of an individual's personal data collected through geolocation and the use of the data in criminal proceedings against him, the court did not find that of Article 8⁸⁵⁴ had been violated (*Uzun v. Germany*, 2010, §§ 60-74). An essential safeguard was provided by judicial scrutiny and the potential for exclusion of data gathered through unauthorized GPS surveillance, which deterred the investigating authorities from gathering data through unlawful methods. (*ibid.*, § 72). Examining the proportionality of the interference also

⁸⁵⁰ For the full guide, see Guide to the Case-Law of the of the European Court of Human Rights, Data protection, Updated on 30 April 2022, available at: https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, (accessed on 23 June 2024).

⁸⁵¹ Guide to the Case-Law of the of the European Court of Human Rights, p.18.

⁸⁵²For the full decision see European Court of Human Rights, *Uzun v. Germany*, 2010 available at: <https://hudoc.echr.coe.int/eng#%7B%22languageisocode%22:%5B%22ENG%22%5D,%22appno%22:%5B%2235623/05%22%5D,%22documentcollectionid%22:%5B%22CHAMBER%22%5D,%22itemid%22:%5B%22001-100293%22%5D%7D> (accessed on 23 June 2024).

⁸⁵³ *Uzun v. Germany*, 2010, §§ 80.

⁸⁵⁴ Article 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01), protection of personal data.

considered the fact that domestic law placed very strict restrictions on the authorization of the contested surveillance measure, that the GPS surveillance was only ordered after less intrusive means of investigation had proven ineffective, and that it had been conducted for a relatively brief period of time (ibid., §§ 77-81).⁸⁵⁵

Also, example related to another kind of approach on location tracking, the guide of the ECHR also mentions *Ben Faiza v. France*, 2018,⁸⁵⁶ case and mentions that in a case where domestic law (neither statute law nor case-law) did not at the relevant time indicate with sufficient clarity as to how, and to what extent, the authorities were permitted to use their discretionary power in this area, the Court found that the decision on the installation of a real-time geolocation device on a person's vehicle in the context of a criminal investigation into drug trafficking violated Article 8.⁸⁵⁷ As seen, long story short, each tracking matter are scattered around geolocation data, yet, within a different context and nature. In other words, although these samples are not dealing with contact tracing applications, it is still possible to derive key takeaways for contact tracing applications. Nonetheless, the outcome that we would like to derive for data controllers of the contact tracing apps is, as discussed in the section, there is not any black-and-white answer for the privacy intrusiveness of location tracking for any kind of processing activities, including digital contact tracing. Accordingly, although we provided an alternative cutting-edge methodology to mitigate any potential privacy intrusiveness of the apps, we pointed out the importance of other factors that come into play, such as abuse of the secure location processing, proportionality and necessity of location tracking and other technical and organisational measures supporting either choice of tracking. Furthermore, the proportionality depends on the duration of the data protection measures, and the ephemeral nature of contact tracing tools, especially those with

⁸⁵⁵ *Uzun v. Germany*, 2010, §§ 77-81.

⁸⁵⁶For the full decision see European Court of Human Rights, *Ben Faiza v. France*, 2018, available at: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-180657%22%7D> (accessed on 23 June 2024).

⁸⁵⁷ Guide to the Case-Law of the of the European Court of Human Rights, p.18.

broader privacy implications such as contact tracing apps, is used as an argument for striking a proper balance between individual rights and the public interest.⁸⁵⁸ Nevertheless, privacy specialists are worried that the additional technological capabilities discovered within the scope of Covid-19 pandemic is going to stay subsequent to the end of the pandemic, as it was happened after the 9/11 attacks in the United States (Bloss, 2007; Levi & Wall, 2004; Sinha, 2013).⁸⁵⁹ Therefore, governments implementing contact tracing measures should ensure the temporary character of the measures in order for them to be proportionate to the aim⁸⁶⁰. Therefore, considering both decisions, it is clearly seen that there are also instances, where location tracking does not seem to be the least privacy-protecting option, whereas at the same time some instances that exactly support the criticisms of the scholars. As such, it supports our idea that there is not any clear-cut risk-free tracking methodology. Rather the act of data controllers should be in line with the GDPR requirements in every phase of the processing activities, as it is detailed in the security of processing and the privacy-by-design section, and the boundaries of utilization of the location data should be interpreted in a way that is in line with the boundaries of data minimization requirement in this Chapter.

Hence, considering these explanations and recommendations, it is plausible to state that efficient data minimization practices implemented by data controllers of the apps have a material impact on the success of location data requirement related to overstretching of the boundaries and narrow interpretation of the use cases. As such, to conclude, although Bluetooth-based applications seem inherently more privacy-friendly options than geolocation data, there are still other options available for tracking, if the required safeguards are implemented. As a good sign, contact tracing

⁸⁵⁸ Van Kolschooten, Hannah, and de Ruijter, Anniek (2020) "COVID-19 and privacy in the European Union: A legal perspective on contact tracing", *Contemporary Security Policy*, vol.41, no. 3, pp. 478-491. p.485.

⁸⁵⁹ Van Kolschooten, Hannah, and de Ruijter, Anniek (2020) "COVID-19 and privacy ...", op.cit., p.485.

⁸⁶⁰ *Ibid.*

applications employed within the EEA are putting an effort to comply with the spirit of the GDPR by using as least as location data possible, and none of them opted for direct location usage except Norwegian application. Having said that, there is requirement to solidify these mechanisms on an ongoing basis due to the novelties and abuses brought by new technologies and tracking methodologies.

2. Security of Processing, Accuracy, Integrity, and Confidentiality

The integrity, confidentiality⁸⁶¹ and accuracy⁸⁶² of the processed data is of massive importance for both data controllers and data subjects, as set out in the GDPR. This necessity is indicated under the Article 5-1-f of the GDPR, and as a complimentary application under the GDPR, personal data must be processed and stored by using appropriate technical or organizational measures to ensure adequate security of processing activities⁸⁶³, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Furthermore, data controllers are also required to mitigate the risks elaborated in Chapter 2 under Data Management and Architecture of the Applications sections in their processing activities. Therefore, it is plausible to state that this part of the thesis consists of wide array complementary aspects regarding the security, integrity, accuracy and storage of personal data, due to the closely connected nature of the topic. Accordingly, as per the Commission's indication, the level of security should typically correspond to both the volume and sensitivity of processed personal data.⁸⁶⁴ Accordingly, it is positive observe that despite such short timeframe to develop the application, many controllers such as Czech, Belgium, Austria, and many others, except Croatia, Cyprus, Malta, Latvia, implemented a participatory processes and stakeholder engagement to ensure certain level

⁸⁶¹ Article 5-1-f of the GDPR, integrity and confidentiality.

⁸⁶² Article 5-1-d of the GDPR, accuracy.

⁸⁶³ Article 32 of the GDPR, security of processing.

⁸⁶⁴ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).

of technical and organizational measures as per the EU Commission report⁸⁶⁵, and their policies. Also some of them have implemented regular checks for data security and privacy, and it is plausible to observe that almost each of them relying on both centralized decentralized architectures utilized the arbitrary ephemeral identifiers.⁸⁶⁶ Likewise, majority of the controllers, i.e. Poland, Croatia, Austria, Lithuania, Italy, Germany, Belgium and etc. also utilized as encryption, pseudonyms identifiers, anonymization, and other techniques.⁸⁶⁷ Therefore, although these are creating some level of technical safeguards, given the countless opportunities to abuse these applications, some of which were detailed in Chapter 2, we need to pinpoint the requirements in light of the current needs that we discovered. To this end, we will further discuss and propose other supportive measures in the following.

To this end, we, first, believe that encryption prerequisites and IT protections, including logical access controls, firewall security, verification and authentication systems, encryption measures, among others, should be implemented by each data controller of contact tracing applications as associated safeguards. Not any identifiable data should be transmitted with any public or private organization.⁸⁶⁸ Pseudonymized or aggregated data holds potential for constructing machine-learning models, epidemiological studies, and guiding public policy. However, data residing on users' devices should remain encrypted and inaccessible to both public authorities and private interests to ensure privacy and security. Particularly, using privacy-

⁸⁶⁵ For the full report see European Commission, Directorate-General for Communications Networks, Content and Technology, Prodan, A., Birov, S., Wyl, V. et al., Digital contact tracing study – Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2759/146050> (accessed on 28 April 2024).

⁸⁶⁶ European Commission Digital Contact Tracing Study on lessons learned (2022), *op.cit.*, p.39.

⁸⁶⁷ For the full details see STOP COVID - ProteGO Safe, *op.cit.* Definitions, Stop Covid-19, privacy policy, *op.cit.*, section 7 application security, The Stop Corona App privacy policy, *op.cit.*, section 4.4., Korona Stop LT' Privacy Policy, *op.cit.*, Section 5.2, Immuni App Documentation, , *op.cit.* Privacy, para 7 and 8, Corona Warn app privacy notice, *op.cit.*, section, 5-e, Coronaalert privacy statement, *op.cit.* section 9.

⁸⁶⁸ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy... ", *op.cit.* p.343.

preserving techniques, the location history could be obscured to achieve some privacy, even for the infected individual.⁸⁶⁹ Therefore, both pseudonymization and anonymization, strongly advocated for by the GDPR, facilitate compliance with its regulations,⁸⁷⁰ and as a positive approach each of the data controllers in EEA/EU indicated that they rely on anonymous processing in entirety of their processing activities. That being said, these techniques should be regularly and widely applied and reviewed due to the evolving re-identification and cyber-attack risks detailed in Chapter 2. Entities handling personal data should employ either method to mitigate risks, with automation potentially reducing the costs associated with compliance efforts.⁸⁷¹

Accordingly, advised by the EDPS, European Institutions must ensure that they safely collect and process only the minimum amount of data and use privacy-friendly technologies at all stages of the process.⁸⁷² This can contain: granting access only on a need-to-know basis to agents trained regarding confidentiality, conducting accountability safeguards regarding data access (e.g. logging), and retaining the contact data on secured servers or on cloud services designed for storing health data⁸⁷³ Also, in addition to the implementation of these measures, the EDPS recommended the necessity of

⁸⁶⁹ Raskar, Ramesh; Dhillon, Ranu; Kapa, Suraj; Pahwa, Deepti; Falgas, Renaud; Sinha, Lagnojita; Prasad, Aarathi et al. (2020) "Comparing manual contact tracing.....", *op. cit.*, p.6.

⁸⁷⁰ Van Schendel, Olenka (2020) "Data masking: Anonymisation or pseudonymisation?", GRC World Forums, available at: <https://www.grcworldforums.com/data-management/data-masking-anonymisation-or-pseudonymisation/12.article> (accessed on 22 June 2024)

⁸⁷¹ Van Schendel, Olenka (2020) "Data masking: Anonymisation or pseudonymisation?", GRC World Forums, available at: <https://www.grcworldforums.com/data-management/data-masking-anonymisation-or-pseudonymisation/12.article> (accessed on 22 June 2024)

⁸⁷² EDPS Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis, available at: https://edps.europa.eu/system/files/2021-02/21-02_02_orientations_on_manual_contact_tracing_euis_en_0.pdf, (accessed on 23 June 2024), p.10 .

⁸⁷³ EDPS Orientations on manual contact tracing., *op.cit.*, p.10.

regular documentation and audit of these above-mentioned measures.⁸⁷⁴ Although this guidance deals with European institutions, agencies, and bodies (EUIs) implementing a manual contact tracing system, and manual contact tracing and digital contact tracing are different⁸⁷⁵, it provides key takeaways from our perspective on digital contact tracing activities for strengthening confidentiality, integrity and accuracy of personal data, given that controllers are the institutions of member states such as ministry of health.

We strongly recommend data controllers of contact tracing applications to implement detailed access controls and retaining the contact data on secured servers or on cloud services designed for storing health data. However, while implementing these security safeguards, data controllers must consider the Article 32-1 of the GDPR⁸⁷⁶, which recommends controllers to consider the state of the art, the costs of implementation and the scope, context, purpose and nature of the processing. Therefore, we believe that the apps must rely on the cutting-edge models for the security of processing with achievable costs. To this end, for instance, in this regard, authenticity could be used by controllers, which is an important criterion and guarantees that the user location data (absolute or relative location data) is not forged.⁸⁷⁷ Furthermore, while relying on this measure, controllers should define strict rules for data security and user information confidentiality.⁸⁷⁸ Excluding confidential,

⁸⁷⁴ EDPS Orientations on manual contact tracing., *op.cit.*, p.10.

⁸⁷⁵ As mentioned by the article published by Raskar, Ramesh; Dhillon, Ranu; Kapa, Suraj; Pahwa, Deepti; Falgas, Renaud; Sinha, Lagnojita; Prasad, Aarathi et al (2020). available at. "Comparing manual contact tracing and digital contact advice." *arXiv preprint arXiv:2008.07325*, pp.1-9, p.1 (abstract) 'Manual contact tracing is a top-down solution that starts with contact tracers at the public health level, who identify the contacts contacts of infected individuals, interview them to get additional context about the exposure, and also monitor their symptoms and support them until the incubation period is past. On the other hand, digital contact tracing is a bottom-up solution that starts with citizens who on obtaining a notification about possible exposure to an infected individual may choose to ignore the notification, get tested to determine if they were actually exposed or self-isolate and monitor their symptoms over the next two weeks'.

⁸⁷⁶ Article 32-1 of the GDPR, security of processing.

⁸⁷⁷ Trivedi, Ameer and Vasisht, Deepak (2020) "Digital contact tracing: technologies, shortcomings, and the path forward." *ACM SIGCOMM Computer Communication Review* 50, no. 4, pp 75-81, p.80.

⁸⁷⁸ Trivedi, Ameer and Vasisht, Deepak (2020) "Digital contact tracing... ", *op.cit.*, p.80.

password-protected data storage and access mechanisms to the system code ought to be subject to elaborate security audits to provide protection against attacks.⁸⁷⁹ As stated by the EDPB, servers involved in contact tracing systems should collect only contact histories or pseudonymous identifiers of users who have been confirmed as infected through proper assessment by health authorities and voluntary actions by users.⁸⁸⁰ Alternatively, the server must retain a list of pseudonymous identifiers or contact history of infected users for a duration adequate to notify potentially exposed individuals, and also, the server should not attempt to identify these potentially infected users.⁸⁸¹ The tracing app can provide notifications to high-risk connections and urge that users notify health authorities willingly where appropriate, greatly assisting in contact tracing while reducing the possibility of state spying, eavesdropping, or vigilantism.⁸⁸² When coupled with other sources of data, the granular non-identifying data used to train machine-learning systems often contains enough detail to re-identify individuals,⁸⁸³ as detailed in Chapter 2. Accordingly, the application's source code and the privacy mechanisms employed should be made public as detailed in different parts of this thesis. Individuals should be able to make independent rational decisions based on the advice provided by the app rather than utilizing coercive or penalizing tactics.⁸⁸⁴ As a positive approach, almost each of the controllers, including but not limited to Italy⁸⁸⁵,

⁸⁷⁹ Trivedi, Ameer, and Vasisht, Deepak (2020) "Digital contact tracing..." *op.cit.*, p.80.

⁸⁸⁰ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

⁸⁸¹ *Ibid.*

⁸⁸² Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy..." , *op.cit.*, p.343.

⁸⁸³ *Ibid.*

⁸⁸⁴ Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy..." , *op.cit.*, p.343

⁸⁸⁵ Immuni App Git Hub Source Code <https://github.com/immuni-app/immuni-documentation> (accessed on 23 June 2024).

Malta⁸⁸⁶, the Netherlands⁸⁸⁷, France, Poland⁸⁸⁸, Iceland⁸⁸⁹, Norway⁸⁹⁰, Portugal⁸⁹¹, Estonia⁸⁹², Cyprus⁸⁹³ provided source code openly, whereas Lithuania and Hungary did not.

Fundamentally, from legal perspective, the safest way is, once the pandemic is over, to delete all application-related personal data from users' phones and from the machine learning server, and to leave only deidentified, aggregated, and statistics or artificial data collected using the epidemiological model, for further research, as implemented by aforementioned controllers, i.e., Norway, Germany, France and etc. By this method, the risk of re-identification delineated under the Chapter 2 could also be mitigated by controllers of the apps. Nevertheless, to be more realistic and pinpoint the real problems, it is important to mention that in some situations implementing a global contact tracing technique that includes both apps and manual tracing may need the retention of extra data, as described in data minimization and purpose limitation sections. In such case, the additional data should be kept on the user's terminal and processed only when absolutely necessary and with his explicit agreement. Since the GDPR is a legal document, many of its requirements are interpretable in the sense that they have to account for

⁸⁸⁶ COVIDAlert Git Hub Source Code <https://github.com/GOVMT-MITA> (accessed on 23 June 2024).

⁸⁸⁷ CoronaMelder Git Hub Source Code <https://github.com/minvws> (accessed on 23 June 2024).

⁸⁸⁸ ProteGO Git Hub Source Code <https://github.com/ProteGO-Safe> (accessed on 23 June 2024).

⁸⁸⁹ Rakning C-19 Git Hub Source Code <https://github.com/aranja/rakning-c19-app> (accessed on 23 June 2024).

⁸⁹⁰ Smittestopp Git Hub Source Code <https://github.com/folkehelseinstituttet/Fhi.Smittestopp.App> (accessed on 23 June 2024).

⁸⁹¹ StayAway Git Hub Source Code <https://github.com/stayawayinesctec/stayaway-app> (accessed on 23 June 2024).

⁸⁹² HOIA Git Hub Source Code [koodivaramu.eesti.ee/tehhik/hoia/documentation](https://github.com/koodivaramu.eesti.ee/tehhik/hoia/documentation) (accessed on 23 June 2024).

⁸⁹³ CovTracer-EN Git Hub Source Code, github.com/CovTracer-EN/covtracer-en-app (accessed on 23 June 2023).

future developments and court decisions.⁸⁹⁴ To elaborate this approach, interpretable nature of the rules is Privacy Engineering Approaches for GDPR Requirements stated as "the appropriate organizational and technological measures" to fulfil a certain privacy property.⁸⁹⁵ To protect data stored in servers and apps, as well as data transfers between applications, state-of-the-art cryptographic algorithms must be applied again to address the re-identification risks detailed in Chapter 2 and fulfil the GDPR requirement, which both secure the integrity and confidentiality of personal data and success of efficient storage limitation. For example, in the context of contact tracing apps, homomorphic encryption, which is a cryptographic method that enables a third party, such as a cloud service provider, to execute specific computations on encrypted data without altering the characteristics of the function or the format of the encrypted data⁸⁹⁶, which also can be used to protect the privacy of individual users by allowing their data to be analysed without being decrypted. This term, homomorphic encryption, seems to be widely used nowadays, in many fields using encrypted data. It brings a unique breakthrough that allows enhanced confidentiality of data without decryption or disclosure of secrets to the server if tampered with by an untrusted server.⁸⁹⁷ Also, it is highly regarded by privacy scholars, as the results of the analysis can then be decrypted without revealing the contents of the original data. One example of a contact tracing app that uses homomorphic encryption is the DP-3T protocol, whose details are provided in Chapter 1. The encrypted data can be analysed without being decrypted, providing effective contact tracing while still protecting user privacy. The fundamental reason is anonymized data is not considered personal information and benefit from

⁸⁹⁴ Huth, Dominik and Matthes, Florian (2019) "Appropriate technical and organizational measures": identifying privacy engineering approaches to meet GDPR requirements", *Americas Conference on Information Systems*, pp.1-10, p.2.

⁸⁹⁵ *Ibid.*, p3.

⁸⁹⁶ Acar, Abbas; Aksu, Hidayet; Uluagac, A. Selcuk; and Conti, Mauro (2018) "A survey on homomorphic encryption schemes: Theory and implementation." *ACM Computing Surveys (Csur)* 51, no. 4, pp.1-35, p.2.

⁸⁹⁷ Carpov, Sergiu, Thanh Hai Nguyen, Renaud Sirdey, Gianpiero Constantino, and Fabio Martinelli. (2016) "Practical privacy-preserving medical diagnosis using homomorphic encryption", *2016 IEEE 9th International conference on Cloud Computing (CLOUD)*, pp. 593-599, p.593.

relaxed standards under GDPR, thus, the need to apply non-reversible masking and anonymization over encrypted data is required.⁸⁹⁸ In this aspect, we can provide certain cutting-edge measures that have been tried by different data controllers within the scope of contact tracing activities, which are in line with the spirit of the GDPR compliance activities.

Likewise, another cutting-edge privacy friendly solution for this particular situation that would be in line with the spirit of the GDPR is multi-party computation (MPC) technique, whose aim is to allow a group of independent data owners, who do not trust each other or any shared third party, to collaboratively compute a function that relies on all of their private inputs.⁸⁹⁹ It facilitates privacy-preserving applications by allowing multiple mutually distrusting data owners to collaborate in computing a function.⁹⁰⁰ Each party locally encrypts its data, and then the encrypted data is combined in a way that allows the desired function to be computed without revealing any of the individual inputs. Secure MPC ensures enhanced privacy, correctness, and independence of inputs, and provides output delivery.⁹⁰¹ One example of a contact tracing app that uses MPC is the COVID Trace app, which was developed by researchers at the University of Toronto. The COVID Trace app uses Bluetooth technology to detect when two users are in close proximity and stores encrypted proximity data on each user's device.⁹⁰² The app uses MPC to compute a function on the encrypted proximity data that allows for contact tracing without revealing users' location data to any party. Another example of a contact tracing app that uses MPC is the DP-3T (Decentralized

⁸⁹⁸ Kesarwani, Manish, Akshar Kaul, Stefano Braghin, Naoise Holohan, and Spiros Antonatos (2021) "Secure k-anonymization over encrypted databases", *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, pp. 20-30, esp. p.24.

⁸⁹⁹ Evans, David; Kolesnikov, Vladimir and Rosulek, Mike (2018) "A pragmatic introduction to secure multi-party computation." *Foundations and Trends in Privacy and Security*, vol.2, no. 2-3, pp. 70-246, p.74.

⁹⁰⁰ *Ibid.* p.75.

⁹⁰¹ Zhou, Jiapeng; Feng, Yuxiang; Wang, Zhenyu and Guo, Danyi (2021) "Using secure multi-party computation to protect privacy on a permissioned blockchain", *Sensors*, vol.21, no. 4 1540, pp.1-17, p.2.

⁹⁰² Covid Trace Application <https://www.covidtrace.org/> (accessed on 23 June 2024).

Privacy-Preserving Proximity Tracing) app, which was developed by a consortium of European researchers. The DP-3T app uses Bluetooth technology to detect when two users are in proximity and stores encrypted proximity data on each user's device.⁹⁰³ The app uses MPC to compute a function on the encrypted proximity data that allows for contact tracing without revealing users' location data to any party, which is preserving act for confidentiality, integrity and accuracy of the personal data. This is also massively supported by scholars, and we believe it is compatible with the term of “cutting-edge” and “cost efficient” set out in the GDPR.⁹⁰⁴

Alternatively, another useful cutting-edge solution in line with the GDPR and ePrivacy Directive requirements would be zero-knowledge proofs (ZKPs) are a cryptographic method enabling one party (the prover) to demonstrate to another party (the verifier) that they possess specific information without divulging any extra details about that information. In other words, zero-knowledge proofs cryptographic techniques could provide privacy for verifying private data without revealing the data in its clear form.⁹⁰⁵ Therefore, ZKP can be used in conjunction with contact tracing apps to enable contact tracing without revealing the user's personal information.⁹⁰⁶

A prominent example of a use case for ZKPs in contact tracing is the TraceTogether app of Singapore⁹⁰⁷. The application utilizes Bluetooth technology to detect when two users are in close proximity and stores encrypted proximity data on each user's device. If a user is diagnosed with COVID-19, they can choose to upload their proximity data to a central server, which can then be used to identify other users who were near the infected user. Furthermore, the study of Liu and colleagues, which examined a privacy

⁹⁰³ See DP3T Website <https://www.dp3t.org/> (accessed on 23 June 2024).

⁹⁰⁴ Article 32 of the GDPR, security of processing.

⁹⁰⁵ Pop, Claudia Daniela; Antal, Marcel; Cioara, Tudor; Anghel, Ionut and Salomie, Ioan (2020) "Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy", *Sensors*, vol. 20, no. 19, 5678, p.5.

⁹⁰⁶ See Git Hub Tripleblind Market <https://github.com/tripleblindmarket> (accessed on 15 August 2022).

⁹⁰⁷ Trace Together Website *op.cit.* (accessed on 15 August 2022).

preserving model for contact tracing applications, they came to the conclusion that using zero knowledge proof, our apps allows the notification of close contacts, without revealing the location and identification of these close contacts (to governments).⁹⁰⁸ Thus, it is a good chance that ZKP method will bring a promising solution for re-identification related risks going forward by enhancing confidentiality and integrity, and security of processing activities within the scope of contact tracing activities. Accordingly, it is plausible to state that the cutting-edge techniques are both in line with the spirit of the European regulatory approach and efficiency of contact tracing applications.

Having said that, the security of processing delineated under the GDPR and ePrivacy directive is not limited with these novel approaches. In other words, to keep acting in line with the legal framework set out by the GDPR, data controllers must ensure the accuracy, integrity, availability and confidentiality of data collected from data subjects⁹⁰⁹ with the efficient organisational measures as well, as set out under the GDPR⁹¹⁰. This means considering and combining the most effective legal, organisational, and technical measures, including advanced statistical and computational safeguards to manage privacy and data protection risks and address ethical issues.⁹¹¹ Otherwise, in case the data in question gets into the possession of unauthorized third party via re-identification methods indicated in Chapter 2, this will cause serious problems in terms of data security, therefore, any potential data security breach would result in breach of special category of personal data, which leads to severe legal consequences for the data controllers. As part of these organisational measures, we are of the view that the most important thing is

⁹⁰⁸ Joseph K. Liu; Man Ho Au; Tsz Hon Yuen; Cong Zuo; Jiawei Wang; Amin Sakzad; Xiapu Luo; Li Li; Kim-Kwang Raymond Choo (2021) "Privacy-Preserving COVID-19 Contact Tracing App...", op.cit., p.2.

⁹⁰⁹ See ICO (2023), "Integrity and Confidentiality" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/> (accessed on 23 June 2024).

⁹¹⁰ See Recital 78 of the GDPR, appropriate technical and organizational measures.

⁹¹¹ Gasser, Urs; Ienca, Marcello; Scheibner, James; Sleigh, Joanna and Vayena, Effy (2020) "Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid", *The Lancet Digital Health*, vol.2, no. 8 pp. e425-e434, p.e431.

to hire subject matter experts for the technical implementation of cyber security and data protection matters, as there might be countless number of risks as articulated in Chapter 2.

For instance, one of the Norwegian municipalities was the target of a drastic cyberattack that took place in January, 2021, in which case employees cannot have access to most of the municipality's IT systems, as the municipality's data was encrypted, and back-ups were erased.⁹¹² Accordingly, The Municipality of Østre Toten's personal data security was found to be seriously and fundamentally defective by the Norwegian Supervisory Authority. Logs and log analytics, backup security, and a lack of two-factor authentication or other comparable security procedures are some of these problems. The firewall was inadequately designed in terms of logging, and most of the internal activity was never logged.⁹¹³ Servers were not designed to send logs to a log centre and failed to log critical events. Besides, the municipality failed to preserve backups from intentional and accidental deletion, manipulation or reading.

Therefore, we consider this sample as a navigator for data controllers of contact tracing applications as well to understand the fact that sometimes classical methods of technical measures could not be sophisticated enough to prevent any sort data breach under the GDPR⁹¹⁴. Our reasoning is, although many advanced technological safeguards were put into place by data controllers of the impacted entity, it is vigilant to implement most-up-to-date solutions, which is in line with the direction GDPR.

⁹¹² For the full description and decision see the EDPB Website, Norwegian SA Issues Fine Municipality Østre Toten for Flawed Information Security https://edpb.europa.eu/news/national-news/2022/norwegian-sa-issues-fine-municipality-ostre-toten-flawed-information_sv (accessed on 23 June 2024).

⁹¹³ For the full statement see Datatilsynet (the Norwegian Data Protection Authority) Stament, Østre Toten Kommune <https://www.datatilsynet.no/contentassets/4609027cf9504e9aa12c3f05b45bdcf7/varsel-om-vedtak-om-overtredelsesgebyr-og-palegg.pdf> (accessed on 23 June 2024).

⁹¹⁴ Article 4-12 of the GDPR, personal data breach definition.

Hence, for data controllers of the apps not to encounter such undesired outcomes as experienced by Norwegian Municipality, the most tailor-made method is to provide due care on cyber security and encryption-related matters as well as hiring specialized task forces specifically devoted to technical and organizational measures, rather than trying to solve the issue with in-house possibilities which are not eligible for this task. To implement a thorough compliance activity for the security of processing, we believe that external company would work in harmony with the in-house counsels of controllers to see any potential data protection and cyber security vulnerabilities of data controllers. The reason is, we believe that it is not always straightforward to deploy all required cutting-edge measures. To this end, from our perspective, it is advisable to deploy a taskforce for cyber security matters for each data controller and regularly communicate with the non-profit European Organisations to enhance these safeguards, such as the European Cyber Security Organisation.⁹¹⁵ Through this way, data controllers keep their agility against evolving risks and thereby having a chance to implement cutting edge measures as in line with the GDPR.⁹¹⁶ Nevertheless, data controller must still consider the every single component of the processing activities of the applications. To put differently, hiring specialized subject matter experts for technological matters would not entirely relieve data controllers from the obligation of compliance with the GDPR security of processing requirements. To this end, it is also important to consider third party stakeholders to the contact tracing activities. we strongly advise to consider all sort of contractual safeguards with third-party suppliers or vendors

⁹¹⁵ “The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO is the privileged partner of the European Commission for the implementation of the Cybersecurity Public-Private Partnership, as well as a recognised actor in the European institutional landscape, A pan European, multi-stakeholder and cross sectoral partnership organisation working on cybersecurity with a holistic approach, ECSO federates the European Cybersecurity public and private sector, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and associations, as well as the local, regional and national public administrations across the European Union Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries.” For the full description see <https://ecs-org.eu/>.

⁹¹⁶ Article 32 of the GDPR, security of processing.

within scope of cyber security activities. This is related to authentication necessities. For instance, with regards to the over-retention risks, which goes hand in hand with the architectural choice of contact tracing apps, conditions and timing of the deletion of centralized data would need to be included in a "sunset clause" for surveillance measures to be in accordance with the notion of being purpose-driven.⁹¹⁷ This is especially pertinent for personally identifiable information. Still, it applies to any data submitted with the understanding that they would only be used for connection tracing or public health monitoring.⁹¹⁸ Where there is a chance that data can be used to enhance the handling of public health crises, which might take place in the future, should declare in advance; at a minimum, data can be re-identified, and a clear and public declaration provided to provide justification for their use at a future date.⁹¹⁹ Having said that the nature of contractual measures, mostly not qualify to be binding the authorities of the country, once they are not party to the contract, these measures should be combined with other technical and organisational measures to provide the level of data protection required.⁹²⁰ The GDPR allows for the use of contractual provisions that provide adequate data protection protections as a justification for data transfers from the EEA to third countries.⁹²¹ Included in this are common contract provisions that have been "pre-approved" by the European Commission. Having said that, we believe that these clauses must not be used as a stand-alone source, rather it should be used in conjunction with the elaborated guidance published by the European Data Protection Board

⁹¹⁷ Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing...", *op.cit.*, p.23.

⁹¹⁸ Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) "Digital contact tracing...", *op.cit.*, p.23.

⁹¹⁹ *Ibid.*

⁹²⁰ Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 Annex 2: Examples of Supplementary Measures, 28.

⁹²¹ See European Commission Website, Standard Contractual Clauses https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on 15 August 2022).

(EDPB).⁹²² In line with this, the EDPB suggests that national health authorities could serve as the controllers for such applications, although other controllers could also be considered.⁹²³ To be more specific, Polish Data Protection Authority imposed a fine on a company for not implementing adequate technical and organizational measures to guarantee the security of personal data and failing to verify the processor.⁹²⁴ The reason is that the personal data breach involved the copying of the controller's customer data by unauthorized persons, due to the changes were made by the processor with which the controller cooperates on the basis of agreements concluded, including the personal data processing entrustment agreement.⁹²⁵ Hence, during its proceedings, the Polish DPA found that the company, in its contractual provisions with the processor, specified the personal data security requirements to be applied. Thus, although the subject matter of the causing details and potential concerns of contact tracing applications within the scope of third-party components are different, as third-party service providers do not act as typical data processors for contact tracing activities, still it brings a useful standpoint for the importance of clear contractual arrangement between contact tracing applications and their third-party service providers.

Also, within the same remit, regarding contracts with subcontractors of data controllers, as mentioned by “Commission Nationale de l'Informatique et des Libertés” (‘CNIL’), selecting a subcontractor which is able to provide sufficient guarantees documenting the means used to ensure the effectiveness of the guarantees offered by the subcontractor in terms of data protection and

⁹²² European Commission Website
https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf (accessed on 15 August 2022).

⁹²³ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.7.

⁹²⁴ For the summary of) ‘the Record fine imposed on controller for personal data breach’ decision see ‘Prezes Urzędu Ochrony Danych Osobowych, (UODO) <https://uodo.gov.pl/en/553/1311> (accessed on 24 June 2024).

⁹²⁵ For the full decision see Prezes Urzędu Ochrony Danych Osobowych, (UODO) Decision DKN.5130.2215.2020 <https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020> (available in Polish) (accessed on 24 June 2024).

signing a contract with the subcontractors, which defines the subject, the length and the purpose of the processing, as well as obligations of each party listed under basic precautions regarding supervising data security with subcontractors.⁹²⁶ Or else, Australian data controller, by using, Privacy Impact Assessment provided recommendations that the Government should confirm the arrangements with AWS (Amazon Web Services) and ensure the contract is sufficient.⁹²⁷ The government has categorically said that the US government cannot access the data through AWS,⁹²⁸ which we believe that, as detailed in Chapter 2, one of the most remarkable concern of the users. Accordingly, we also believe that European contact tracing applications can benefit from the same logic while dealing with third-party engagements as a contractual safeguard, as part of their organizational measures. Implementation of the contractual solutions for stipulating the third-party actions could radically reduce the risk of poor data security management implemented by the third-party involvement, and drastically diminish the risks regarding data management activities delineated in Chapter 2.

Similarly, another organizational safeguard is, as mentioned above, designating a data protection officer, because the processing event is implemented by a public authority other than the courts that are acting in their judicial capacity, pursuant to Article 37-1-a of the GDPR ⁹²⁹ as necessity for data controllers. The reason is organizational measures could correspond to the adoption of specific procedures and the selection of certain individuals to decide and action on several aspects of data processing, including the type of privacy-enhancing technologies to be utilized through the data sharing and

⁹²⁶ For the details and further information see CNIL's Guide, Security of Personal Data. 2018, p.19 https://www.cnil.fr/sites/default/files/atoms/files/guide_security-personal-data_en.pdf . (accessed on 23 June 2024).

⁹²⁷ Norton Rose Fulbright, (2020) Contact Tracing Applications in Australia, op.cit., p.1.

⁹²⁸ Norton Rose Fulbright, (2020) Contact Tracing Applications in Australia, op.cit., p.1.

⁹²⁹ Article 37- 1- a of the GDPR, Designation of the Data Protection Officer.

reusage lifecycle.⁹³⁰ Accordingly, the necessity for specific information about data controller identity must be covered in the website privacy policy of the data controller as per the GDPR, as detailed in the transparency part of the next chapter. Additionally, due diligence process could also be an efficient tool under the organisational measures. The reason is controllers may be held liable in case controller engaging with a processor which cannot guarantee that they have implemented suitable technical and organizational measures to ensure the security of personal data.⁹³¹ It is critical to establish due diligence checks before controller engaging a processor relation and to implement checks on regular basis to ensure processors comply with their obligations.⁹³² In other words, when selecting third-party vendors, conducting due diligence and comparing results can help streamline the search for the ideal controller.⁹³³ In addition, if a vendor experiences a data breach affecting your data or systems, a strong due diligence process can demonstrate that you took necessary measures while choosing vendors, potentially easing scrutiny from regulators.⁹³⁴ Contact tracing applications should also the certain due diligences for the selection of third-party service or product providers within the scope of contact tracing applications to avoid such risk of non-compliance with the article 32 of the GDPR. It is also connected with the measures mentioned by French Data Protection Authority CNIL in its guidance, as explained before.⁹³⁵ A statement regarding the positive evaluation of the due diligence process for the selected third-party vendors on

⁹³⁰ Stalla-Bourdillon, Sophie; Thuermer, Gefion; Walker, Johanna; Carmichael, Laura and Simperl, Elena (2020) "Data protection by design: building the foundations of trustworthy data sharing", *Data & Policy*, vol.2, pp.E4-5.

⁹³¹ Elisavet Dravalou (2021) What "technical and organisational measures" actually means, DP Organizer Website Blog available at: <https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/> (accessed on 22 June 2024).

⁹³² *Ibid.*

⁹³³ See DPO Centre (2020), Due Diligence <https://www.dpocentre.com/vendor-due-diligence-what-you-need-to-consider/> (accessed on 20 June 2024).

⁹³⁴ *Ibid.*

⁹³⁵ For the details and further information see CNIL's Guide, Security of Personal Data. 2018, p19 https://www.cnil.fr/sites/default/files/atoms/files/guide_security-personal-data_en.pdf (accessed on 23 June 2024).

the website and applications statement could also provide another benefit regarding the protection of the personal data of the users, and it would augment the user's trust.

Hence, to conclude, based on the privacy policies, terms and conditions and technical specifications, where available, of contact tracing applications, data controllers of contact tracing applications applied certain security methods to comply with these requirements set out under the GDPR, such as encryption, pseudonyms identifiers, logging, access controls and restrictions, data backup etc. However, due to the evolving nature of the processing activities and potential infectious diseases, these measures should be revisited and updated regularly considering the aforementioned discussions, particularly considering the swift development phase of the applications. Till date, there have not been many major personal data breaches other than a few instances highlighted in this thesis. Nonetheless, still, in addition to these efforts, consulting with the cyber security organizations as well as external vendors for the due diligence process of the third-party engagements should be implemented on an ongoing basis. Through these efforts, it is possible to have more state of art safeguards could be deployed by the controllers to mitigate any potential technical organizational-related risk of contact tracing activities. As detailed in this section, there are many tailor-made novel solutions can be created. Nevertheless, the most important thing is to adjust these novelties into the spirit of the GDPR, as detailed above.

3. DPIA Requirement

The necessity of implementing a data protection impact assessment ('DPIA') is set out under the article 35 of the GDPR.⁹³⁶ Furthermore, as per the Article 9(2)(h), the GDPR adopted expected large-scale adoption, systematic

⁹³⁶ See Article 35 of the GDPR, data protection impact assessment.

monitoring, and use of new technology solutions.⁹³⁷ Particularly, the DPIA process is the key component of the determination and mitigation of the risks mentioned in Chapter 2. A core component of the GDPR is the risk-based approach aims to tackle the challenges posed by new technologies and intricate services that handle personal data,⁹³⁸ considering that instances are the Internet of Things (IoT), mHealth, and mobility applications in which various sensors and Artificial Intelligence (AI) perspective are being utilized for contact tracing activities.⁹³⁹ In particular, special categories of personal data as categorized under the article 9 of the GDPR are routinely processed, particularly in the context of mHealth apps.⁹⁴⁰ Such services frequently include items from many technology vendors (hardware and software artifacts), as well as cloud services from different providers. Hence, data controllers of contact tracing applications must scrutinize their data processing activities by engaging in DPIA before starting data processing activities. The main reason for this necessity is that in case of high-risk processing, such as any health related data processing, data protection impact assessments would most probably deemed mandatory.⁹⁴¹ In addition,

⁹³⁷ Article 9(2)(h) of the GDPR sets out that “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3”.

⁹³⁸ Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) “Data Protection Impact Assessments in Practice” In European Symposium on Computer Security. ESORICS 2021 International Workshops. Lecture Notes in Computer Science, vol 13106. Springer, Cham. https://doi.org/10.1007/978-3-030-95484-0_25, pp.424-443, p.424.

⁹³⁹ Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) “Data Protection Impact Assessments...” *op.cit.* p.424.

⁹⁴⁰ Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) “Data Protection Impact Assessments...” *op.cit.* p.424.

⁹⁴¹ With regards to samples for the potential high-risk processing activities that might be triggering DPIA requirement, see the EDPB (2021) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, p.11. In this section, a hospital managing its patients' genetic and health information (hospital information system) is deemed to be sensitive data or data of a highly personal nature, which therefore would likely to trigger a DPIA as per the guideline.

it is also important to note that the DPIA process is the fundamental part of a “privacy by design” perspective, which assists organizations fulfil the privacy and data protection expectations of their customers, employees, and other stakeholders.⁹⁴²

Therefore, considering the above introduction, in this particular instance, DPIA must also be implemented by the data controllers of the applications as per the Article 29 Data Protection Working Party propositions, which set forth several criteria that serve to define technologies as constituting a high-risk in terms of severity of privacy risks, such as evaluation and scoring, automated decision making with legitimate or similar noticeable impact, systematic monitoring, sensitive data, data processed on a massive scale).⁹⁴³ With regards to the components of DPIA of any controller, including but not limited to contact tracing applications, an ideal DPIA should contain the following⁹⁴⁴;

- context, nature, scope as well as purposes of potential data processing activity,
- evaluate the necessity, proportionality, and compliance measures to be employed during potential data processing activity,
- identify and evaluate risks that might be imposed on individuals,
- determine any additional precautionary measurements to mitigate any potential risk at stake.

Accordingly, as for the determination of the cases required DPIA process, not to create any room for doubt, the binding Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the

⁹⁴² Georgiou, Dimitra, and Lambrinouidakis, Costas (2021) "Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations", *Future Internet*, vol.13, no. 3, pp. 1-12, p.11.

⁹⁴³ See Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

⁹⁴⁴ See ICO (2023), “Data Protection Impact Assessment” available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#:~:text=A%20Data%20Protection%20Impact%20Assessment,some%20specified%20types%20of%20processing>. (accessed on 23 June 2024).

processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) that sets forth DPIA is required when, among others, location data and health data is at stake.⁹⁴⁵ The opinion of The Dutch Data Protection Authority provides a useful guideline for the processing activities that contain certain types of data, and therefore it is also useful to identify the risks associated with contact tracing applications, although the opinion was not directly associated with the contact tracing applications. Likewise, Polish Data Protection Authority also published the list of processing activities that require DPIA, which also contains, among others, geolocation data and health data.⁹⁴⁶ To this end, the EDPB considers that DPIA should be conducted before deploying such a tool because the processing is likely to be high risk (health data expected to be adopted on a large scale, systematic monitoring, and use of modern technological solution).⁹⁴⁷

Therefore, as seen, regulators also take steps to mitigate any doubt related to the implementation of the DPIA process by data controllers. Having said that, as a common feature of their decisions and acts, they always point out the different and novel means of processing activities. In line with this approach, we believe that the notion introduced by Raab, namely surveillance impact assessment, could be an efficient starting point for controllers of contact tracing applications as well.⁹⁴⁸ Our reasoning is, as per the study, the regulation of surveillance has as one of its main objectives the safeguarding of trans-individual social values, in addition to individual privacy values, and therefore surveillance impact assessment could play a valuable role by incorporating DPIA but transcending it with a range of inquiries aimed at

⁹⁴⁵ For the full list see Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) available at: https://edpb.europa.eu/sites/default/files/decisions/nl_2020-09-02_-_dpa_list_nl_sa_-_national_decision_en.pdf. (accessed on 23 June 2024).

⁹⁴⁶ For the full list see proposed list of types of processing, referred to in Article 35(4) published by Polish Data Protection Office (UODO) available at: <https://uodo.gov.pl/en/558/939>.

⁹⁴⁷ *Ibid.*

⁹⁴⁸ Raab, Charles D. (2020) "Information privacy, impact assessment, and the place of ethics", *Computer Law & Security Review*, n. 37, 105404, pp.1-16, p.9.

assessing the impact of surveillance upon society itself: upon privacy but also upon the other, non-privacy, collective interests of individuals, categories, and groups.⁹⁴⁹ What an innovation, a new database, or a new audio-visual scheme for monitoring public places or private shopping precincts, or the texture of social interactions, is a potentially fruitful line of inquiry that could become institutionalized as a set of practices and requirements before those surveillance possibilities are implemented, or even as a way of amassing evidence for opposing and cancelling some planned developments.⁹⁵⁰ It is an important perspective when evaluating the risks associated with surveillance technologies, from which controllers of tracking technologies can benefit too. Arguably, we believe that as a key takeaway from this approach, due to the similar nature of contact tracing activities, surveillance activities are dynamic and required tailor-made analysis, which comprise its own notions and nuances. Therefore, it is not logical to limit the nature of DPIA with a classical approach. These tailor-made type assessments, could be even more successful in efficiently capturing the risks related to digital contact tracing activities, it is performed as early as possible in the design of the processing activity.⁹⁵¹ It may not be possible to perform a DPIA at the earliest phase of the project, as project goals and some understanding of how the project is going to operate has to be identified before it will be possible to evaluate the data protection risks contained and for some projects DPIA can be a continuous process, and be updated as the project advances.⁹⁵² The main reason for this is the constant change of Covid variants and the increasing prevalence of the virus, resulting in a greater need for these applications. This

⁹⁴⁹ Raab, Charles D. (2020) "Information privacy, impact assessment...", *op.cit.*, p.10.

⁹⁵⁰ Raab, Charles D. (2020) "Information privacy, impact assessment...", *op.cit.*, p.10.

⁹⁵¹ See Data Protection Website, Data Protection Impact Assessments <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=The%20DPIA%20should%20be%20carried,design%20of%20the%20processin%20operation> (accessed on 23 June 2024).

⁹⁵² See Data Protection Website, Data Protection Impact Assessments <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=The%20DPIA%20should%20be%20carried,design%20of%20the%20processin%20operation> (accessed on 23 June 2024).

means that these contact tracing applications will need more diverse data, or longer storage of the same data as detailed in Chapter 3. Accordingly, DPIAs to be made will provide an oversight to the data controller on processing activities planned and any potential feared events as well as risks associated with processing activities.

Additionally, it is important to note that data protection cannot be achieved solely through technology and therefore cannot be assessed through a purely technological analysis of IT components alone.⁹⁵³ The risks associated with the activities of both responsible parties and contracted service providers need to be identified throughout the entire processing chain. Measures to reduce these risks should be proposed, discussed, and evaluated. To establish a quality standard, a DPIA report should conform to the principles of Article 5 GDPR and meet the data protection objectives.⁹⁵⁴ As such, it is fair to state that data controllers of contact tracing applications must vary such detrimental case scenarios for both them and the data subjects. They should follow the above-mentioned necessities when they perform DPIA for contact tracing applications.

Having said that, to go even one step further, we believe that these DPIAs must not be only limited to the processing activities themselves, but also other environmental factors that play a role into the processing activities of contact tracing apps. For instance, potential risks associated with third-party vendors of contact tracing data controllers are indicated in Chapter 2. Data controllers of contact tracing applications map out their routes in case any potential feared event arises due to processing activities. As mentioned under the Chapter 1, there is an important feature of the Croatian contact tracing

⁹⁵³ Rehak, Rainer; Kühne, Christian R. and Bock, Kirsten (2022) "Analysis and Constructive Criticism of the Official Data Protection Impact Assessment of the German Corona-Warn-App", *Annual Privacy Forum*, pp. 119-134, Springer, Cham, p.133.

⁹⁵⁴ Rehak, Rainer; Kühne, Christian R. and Bock, Kirsten (2022) "Analysis and Constructive Criticism...", *op cit.*, p.133.

application, which provides “third-party components” and “DPIA”⁹⁵⁵ to the users. This is an important action to provide transparency and trust, in addition to the necessities mentioned under the previous heading. The issue as to which software tools are included in the process, especially given in the third-party components section, constitutes an example of transparency and trust. Correspondingly, as detailed by Vemou and Karyda in their study where they critically evaluated generic PIA methods suggested in related research, analyzing privacy risks from the organizational standpoint contributes to a comprehensive understanding of induced risks and encourages more conscientious efforts to address or avert privacy risks.⁹⁵⁶ For this reason, PIA methods should explicitly suggest reviewing the roster of implicated personal data in each risk mitigation phase. Particularly, as a useful real-life sample, Italian DPA, Garante, provided The Guarantor for the protection of personal data has authorized the Ministry of Health to start processing related to the Immuni app, on the basis of the impact assessment transmitted by the Ministry.⁹⁵⁷ However, Taking into account the complexity of the alert system and the number of subjects potentially involved, the Garante decided to give a series of measures aimed at strengthening the security of the data of the people who will download the app, particularly increasing the level of detail on the risks on data subject rights.⁹⁵⁸

Correspondingly, we believe that that controllers of contact tracing applications’ perspective should provide a contribution toward a holistic view

⁹⁵⁵ Stop-Covid-19 Application, DPIA https://www.koronavirus.hr/uploads/Stop_COVID_19_Data_Protection_Impact_Assesment_Summary_2020_11_16_58dea76816.pdf (accessed on 23 June 2024).

⁹⁵⁶ Vemou, Konstantina and Karyda, Maria, (2018) "An Evaluation Framework for Privacy Impact Assessment Methods", MCIS 2018 Proceedings, n.5, <https://aisel.aisnet.org/mcis2018/>, pp.1-10, p.8.

⁹⁵⁷ For the full decision of Garante (Italian Data Protection Supervisory Authority), see App "Immuni": via libera del Garante privacy <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9356588> (accessed on 23 June 2024).

⁹⁵⁸ For the full decision of Garante (Italian Data Protection Supervisory Authority), see App "Immuni": via libera del Garante privacy <https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9356588> (accessed on 23 June 2024).

of the risks as well. To this end, in practice, to be more systematic and holistic, data controllers of contact tracing applications should structure their DPIAs, as “umbrella DPIAs” and “addenda to the umbrella DPIAs” or “individual DPIAs”. As mentioned by Friedewald, and colleagues, as services have raising complexity, controllers need elaborate information regarding a service to conduct a DPIA.⁹⁵⁹ Hence, the DPIA methodology proposed by the Government of the Netherlands contains a so-called umbrella DPIA in which service providers conduct a general DPIA that could later be utilized as a basis for individual risk assessments based on a particular context.⁹⁶⁰ This idea is quite useful and valid for contact tracing applications. The fundamental reason why we believe it is important that the practical benefit of such division of DPIAs within the contact tracing domain could be that while ‘umbrella DPIAs’ deal with more generic and radical privacy and security threats to the contact tracing activities, these addendums to be drafted could examine the several different threats that arise more often as per the nature of the processing activities, and it would also grant controllers the required flexibility for detecting threats and acting thereupon. Also, publishing the full list and details of such varied addendums in addition to the umbrella DPIAs could be efficient way to point out the risks for the design process and for ongoing technical and organization measures and gain the trust of the users as well. As advised by the WP29, it is in particular a good practice to publish a DPIA in which cases members of the public are impacted by the processing operation.⁹⁶¹ This could specifically be the case in which a public authority performs a DPIA. Similarly, German Authority, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) DPIAs of the applications should be essentially

⁹⁵⁹ For the full paper see Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) "Data Protection Impact Assessments in Practice" In. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106, Springer, Cham. https://doi.org/10.1007/978-3-030-95484-0_25, pp. 424-443.

⁹⁶⁰ Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) 'Data Protection Impact Assessments in Practice...', *op.cit.*, p.424.

⁹⁶¹ Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/67, p.17.

published.⁹⁶² Therefore, it would bring a useful tool to solidify the trust of the users. On the top all of that, to get back to umbrella DPIA discussion, it is quicker to implement such methodology from controllers' perspective as well, which is in line with the logic provided by the GDPR, in terms of frequent implementation of the DPIAs. So, it would create win-win situation for both data controllers and data subjects.

Subsequently in order to have a deep-dive into the trigger points of DPIA and user risk awareness, a holistic privacy risk assessment framework based on contextual integrity, that practitioners can use to inform decision-making around the privacy risks of contact tracing apps.⁹⁶³ By using the DPIA framework, also provides organizations with a means of assessing privacy from both the perspective of the organization and the individual, thereby facilitating GDPR compliance. We believe that in addition to the aforementioned mandatory requirements, it is important to point out that in order to assist considerations about the nature, sources, and intensity of the risk within the scope of DPIA, the controller must include data subjects in the procedure where appropriate and provide the individuals affected with an opportunity to express their views on the envisaged processing (Article 35(9) GDPR), as also proposed by Bieker and colleagues.⁹⁶⁴ The necessary and proportionality of the process in relation to its purposes, as well as the risks to the rights of the people involved, could be assessed using this information in accordance with Article 35(7)(b) and (c) GDPR.⁹⁶⁵ Within this context, the study of Bieker indicated that among randomly selected participants, some would have more experience in risk assessment than others, whereas some

⁹⁶² For the full decision of the BFDI see Datenschutz bei Corona-Warn-App ausreichend https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/12_Corona-Warn-App.html (accessed on 23 June 2024).

⁹⁶³ For the full article see Henriksen-Bulmer, Jane; Faily, Shamal and Jeary, Sheridan (2020) "DPIA in context: applying dpia to assess privacy risks of cyber physical systems", *Future internet*, vol.12, no. 5, 93, pp. 1-24, p.1.

⁹⁶⁴ Bieker, Felix; Friedewald, Michael; Hansen, Marit; Obersteller, Hannah and Rost, Martin (2016) "A process for data protection impact assessment under the European general data protection regulation", *Annual Privacy Forum*, Springer, Cham, pp. 21-37, p.25.

⁹⁶⁵ *Ibid.*

of the participants had significant risk knowledge and understanding, although this was thought to relate more to security risk rather than privacy risk. Thus, considering this sample, what we can derive for the contact tracing applications is the importance of risk awareness among the group.⁹⁶⁶ As delineated in this section, because risk awareness and appetite might differ among members, consulting with experts, stakeholders, and scholars in the field is more important now to implement efficient risk identification mechanism. This is not only due to the fact that it will entail the situation in which both user trust and security of these applications are to reach the peak level, and important to address the risk of user distrust detailed in Chapter 2, but also the fact that DPIA can be examined as early warning systems that aim to identify the impact of potential risks, and also to fairly balance and mitigate the potential risks with a clear connection to the accountability principle.⁹⁶⁷ Indeed, it is in line with what Recital 84 of the GDPR sets out, namely when choosing the relevant steps to take to show that the processing of personal data implicitly highlights the responsibility of the data controller within the context of the DPIA procedure, the assessment's findings should be taken into consideration. To this end, we believe that the fairness concept and risk resulting from processing activity have a close tie, considering that fairness then manifests itself in the implementation of the rights and requirements provided by the framework to ensure a fair personal data processing ecosystem⁹⁶⁸, which we believe is strictly connected to the users' risk perception about the protection of their rights within the framework of the GDPR. The more the users think about the fairness of processing, in which the DPIA process plays a huge role to determine the risks of processing activity at stake, the less the users feel worried about the processing. Therefore, including data subjects, and other stakeholders to the DPIA

⁹⁶⁶ Bieker, Felix; Friedewald, Michael; Hansen, Marit; Obersteller, Hannah and Rost, Martin (2016) "A process for data protection ...", *op.cit.*, p.25.

⁹⁶⁷ For the full article see Kasirzadeh, Atoosa, and Clifford, Damian (2021) "Fairness and Data Protection Impact Assessments", *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 146-153, p.149.

⁹⁶⁸ *Ibid.*

process would even solidify the robustness of the processing activity. Within the similar vein, Kasirzadeh and Clifford points out another important component of the DPIA process, which could be valid for the controllers of contact tracing applications within the scope of their compliance activities with the GDPR requirements.⁹⁶⁹ That said, in light of these risk awareness of data subjects, and accountability concerns of data controllers, which we believe are also the motivations to engage in DPIA, there is a need to consider the consultation with different stakeholders of contact tracing applications during the privacy impact assessment process,⁹⁷⁰ in order to enhance the level of accountability for risk determination activities. In other words, engaging stakeholders, including the public stakeholders, can assist the assessor of privacy risk assessment to find out the risks and impacts which they might not otherwise consider.⁹⁷¹ Similarly, Hopeman is also supportive of this perspective, as per his research data protection authorities and other stakeholders (including representatives from civil society) could be consulted during developing the entire system.⁹⁷²

The fundamental reason of a consultation is a way to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks. Feedback received and any alterations made to a project as an outcome of stakeholder engagement ought to be included in the privacy impact assessment report.⁹⁷³ Accordingly, as per the EU data, many controllers such as Cyprus, Finland, Austria, Denmark Netherlands, Germany and others consulted with multiple different stakeholders for their DPIA.⁹⁷⁴ We

⁹⁶⁹ Article 5 of the GDPR, principles relating to processing of personal data.

⁹⁷⁰ For the full article and discussions see Wright, David (2013). "Making privacy impact assessment more effective", *The Information Society*, vol.29, no. 5, pp 307-315.

⁹⁷¹ Wright, David (2013) "Making privacy impact assessment...", *op. cit.*, p.311.

⁹⁷² Hoepman, Jaap-Henk (2021) "Hansel and gretel and the virus: Privacy conscious contact tracing." *arXiv preprint arXiv:2101.03241*, pp.1-29, p.14.

⁹⁷³ Wright, David (2013) "Making privacy impact assessment...", *op. cit.*, p.311.

⁹⁷⁴ European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices....." *op.cit.*, p.129-165.

believe, another way of conducting such detailed consultation could also be found in the disclosing the DPIA for further improvement, given that DPIA is an ongoing process. Accordingly, in line with our perspective regarding the publication of results of the DPIA to the public, which is being done by several data controllers including but not limited to controller of Irish app⁹⁷⁵, Polish app,⁹⁷⁶ Latvian app⁹⁷⁷, Croatian app⁹⁷⁸, Netherlands app⁹⁷⁹, and etc., although not all of them shared the full DPIA, it is an efficient way to make the users and public authorities included in the process, which can end up in a situation where increased trust of users gained and they feel have more control over their personal data as in line with the GDPR. Furthermore, since the design of proximity tracking applications was determined by G(apple) to enforce the purpose and nature of processing, this makes G(apple) a joint controller with healthcare authorities regarding the data processing carried out by these applications.⁹⁸⁰ Similarly, establishing a procedure to involve and consult stakeholders can aid policy-makers, technology developers, and project managers in identifying, discussing, and addressing ethical concerns, ideally at the earliest stages of project development.⁹⁸¹

Such situations require GAEN to fulfil its legal obligation to conduct a DPIA concerning the processing aspects under their control, which, for sure, does

⁹⁷⁵ See HSE DPIA <https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%202026.06.2020.pdf> (accessed on 23 June 2024).

⁹⁷⁶ See Protego-Safe DPIA <https://www.gov.pl/web/protegosafe/dokumenty> (accessed on 23 June 2024).

⁹⁷⁷ See Smittestop DPIA https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (accessed on 23 June 2024).

⁹⁷⁸ See StopCovid DPIA https://www.koronavirus.hr/uploads/Stop_COVID_19_Data_Protection_Impact_Assesment_Summary_2020_11_16_58dea76816.pdf (accessed on 23 June 2024).

⁹⁷⁹ See Corona Melder DPIA <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlbqlspueffm> (accessed on 23 June 2024).

⁹⁸⁰ Duarte, Tatiana. (2022) "Google and Apple Exposure Notifications System: Exposure Notifications or Notified Exposures?", *Annual Privacy Forum*, pp. 99-118, Springer, Cham, p.111.

⁹⁸¹ Wright, David, Mordini, Emilio (2013) 'Privacy and Ethical Impact Assessment', *op. cit.*, p.402.

not imply that public healthcare authorities are exempt from conducting a DPIA. Optimally, GAEN and healthcare authorities ought to develop their DPIAs together, or, more actually, the latter should build its DPIA on the one implemented by the former.⁹⁸² Furthermore, stakeholders can provide novel information that the project manager might not have previously considered, offering valuable suggestions for resolving intricate issues.⁹⁸³ Hence, we concur with this perspective as in practice, considering the importance of the public benefit being derived from contact tracing applications, it would be more realistic as well as practical to develop a DPIA together. By this, as detailed above, the risk of negligence pertaining to unchartered risks related to contact tracing applications could be completely mitigated. Moreover, for a DPIA to be credible the other feature that is necessary is that there be some “independent component”. Typically, a satisfactory degree of independence can be obtained by having the PIA undertaken by a paid professional who, while subject to some direction from the proponent as to such matters as timing, operates in an independent fashion. A consultant with appropriate privacy expertise will sufficiently value his or her continuing reputation to offer objective and credible comments and recommendations. From this perspective, the credibility of DPIAs of contact tracing applications could be augmented via the involvement and contribution of privacy experts or scholars with a huge reputation in the field. This would entail the positive perception of the public about the security of contact tracing applications, and early caption of any potential detrimental risks delineated in Chapter 2 with a robust mechanism, which would be resulted from the magnificence of stakeholders’ collaboration, and quite in line with the spirit of the GDPR.

In conclusion, many aspects of the privacy or data protection impact assessments are evaluated under this section. Accordingly, tailor-made solutions provided for controllers. It would be beneficial to mention the frequency of DPIA conducted by data controller in the privacy notice supplied to data subjects as well as privacy policy stipulated on the website of contact

⁹⁸² Duarte, Tatiana. "Google and Apple... ", *op. cit.*, p11.

⁹⁸³ Wright, David, Mordini, Emilio (2013) 'Privacy and Ethical Impact Assessment', *op. cit.*, p.402.

tracing applications. Furthermore, it is significant to consider the feedback provided by other stakeholders in the published DPIA. Similarly, receiving the opinions of the experts in the field is also a credible action for the DPIAs. By this, the level of trust of data subjects could be positively affected, as clear attitude of the data controller against the risk management related matters could be indicated thereby. Furthermore, classifying the generic risks as well as privacy risks, therefore umbrella DPIAs and individual DPIAs could be efficient strategies to enhance the efficiency of risk mitigation activities or privacy by design activities to be implemented by data controllers of tracing applications. All these efforts could result in increased level of trust for users, and more amount of use of contact tracing applications and thereby less amount of positive infected cases. That being said, only very few of controllers published their DPIAs to public. The nations that released their DPIAs include Spain, Denmark, Austria, Finland, Belgium, France, Ireland, Germany, Poland, Norway, Portugal, as per the EU Commission data.⁹⁸⁴ Latvia, Italy, Malta, Slovenia, Lithuania, Croatia, and Iceland either did not publicly disclose their assessments or only provided them in summary form.⁹⁸⁵ Therefore, we believe that there is a room for the improvement in this regard for the future use for the more dynamic and compliant DPIA.

4. Privacy-by-design:

Privacy-by-design method is essential for mitigating the risks from the source of risks delineated in the Chapter 2. To this end, any unrelated or unnecessary data, such as messages, communication IDs, civil status, equipment directory entries, call logs, location data, device identifiers, and so on, should not be collected by the applications.⁹⁸⁶ In other words, data protection by design is referring an approach that provides data controllers consider privacy and data

⁹⁸⁴ European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices...”, op.cit., p.36.

⁹⁸⁵ *Ibid.*

⁹⁸⁶ ICO, Data Protection by design and default available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> (accessed on 23 June 2024).

protection matters starting from the design step of any system, product, service, or process and at the same time during the lifecycle, whereas data protection by default requests controllers to provide that data controller solely process data which is deemed necessary to perform a such specifically defined purpose.⁹⁸⁷ Therefore, privacy by design is an adjuvant for all types of IT systems intended or utilized for personal data processing.⁹⁸⁸ It should be a critical necessity for third-party and individual client products and services (e.g. Wi-Fi routers, search engines, and social networks). Accordingly, this section of the thesis is investigating cutting-edge methods for controllers of contact tracing applications in line with the spirit of the article 32 of the GDPR.⁹⁸⁹

As the reflection of the privacy-by-design on contact tracing apps, complying with the principles of successful data protection and privacy-by-design is crucial in convincing target populations to download and utilize digital contact tracing applications.⁹⁹⁰ In other words, the principle of Privacy by Design supports the idea that privacy should be deemed as a first class citizen in the technology design and ought be intensely inserted.⁹⁹¹ Therefore, as mentioned by the WHO with regards to the design of the applications, important data protection principles such as informed consent, data minimization and purpose limitation should be thoroughly implemented.⁹⁹² Furthermore, any data processed must not contain the identity or

⁹⁸⁷ Information Commissioner's Office Article, Data Protection by design and default available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> (accessed on 15 August 2022).

⁹⁸⁸ Schaar, Peter (2010), "Privacy by Design", *IDIS*, vol.3, pp. 267–274, p.267.

⁹⁸⁹ Article 32 of the GDPR, security of processing.

⁹⁹⁰ O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; et al. (2021) "Best Practice Guidance for Digital Contact Tracing ...", *op.cit*, p.2.

⁹⁹¹ Besik, Saliha Irem, and Freytag, Johann-Christoph (2020) "Managing Consent in Workflows under GDPR...." *op.cit*, p.19.

⁹⁹² WHO, (2020) "Indicator framework for the evaluation of the public health effectiveness of digital proximity tracing solutions" ISBN 978-92-4-002835-7 (electronic version) p.3.

geographical coordinates of a data subject.⁹⁹³ Correspondingly, we are of the view that risk-based approach helps data controllers to foresee any sort of problems arising from the DPIA implemented. Therefore they can embed such safeguards into design of the specific product subject to privacy compliance by utilizing the most cutting-edge privacy-enhancing technologies.⁹⁹⁴ In other words, as stated by the ICO and mentioned in the previous section, DPIAs are an integral part of data protection by design and by default, and privacy-enhancing technologies are attached to the concept of privacy by design, and therefore apply to the technical measures a controller implements.⁹⁹⁵ To this end, as seen below, there are multiple and endless privacy-preserving technologies, that are also in line with the spirit of the ePrivacy Directive, and the GDPR perspective could be derived for contact tracing applications.

First of all, it is important to note that privacy risks associated with data regarding identifiable individuals can be mitigated in great part by using de-identification techniques in conjunction with reidentification procedures.⁹⁹⁶ These strategies can reduce the danger of unintentional disclosure and re-identification while preserving the excellent quality of the data (a key to usability nonetheless, sophisticated and rapid technical progress (e.g., developing analytics) may have unintended privacy consequences; for instance, more effective analytics may mistakenly allow individuals to be re-

⁹⁹³ WHO, (2020) "Indicator framework for the evaluation of the public health effectiveness of digital proximity tracing solutions" ISBN 978-92-4-002835-7 (electronic version) p.3.

⁹⁹⁴ As per the Royal Society Website, "Privacy Enhancing Technologies (PETs) are a suite of tools that can help maximize the use of data by reducing risks inherent to data use. Some PETs provide new tools for anonymization, while others enable collaborative analysis on privately-held datasets, allowing data to be used without disclosing copies of data" [https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/#:~:text=Privacy%20Enhancing%20Technologies%20\(PETs\)%20are,without%20disclosing%20copies%20of%20data](https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/#:~:text=Privacy%20Enhancing%20Technologies%20(PETs)%20are,without%20disclosing%20copies%20of%20data) (accessed on 5 December 2022).

⁹⁹⁵ See ICO Website, Data Protection by design and default, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/?q=DPIA#dpd10> (accessed on 23 June 2024)

⁹⁹⁶ Cavoukian, Ann, and Jonas, Jeff (2012) "Privacy by Design in the Age of Big Data". Eurocontrol Int, pp.1-17., p.8.

identified across vast data sets.⁹⁹⁷ Therefore, privacy should ideally be built in by default during the process's architecture, design, and construction, in particular with respect to the storage of persona data in line with the GDPR principle⁹⁹⁸. For instance, proposals like DP-3T have an automatic mechanism for the deletion of data from the server and the users after a certain period,⁹⁹⁹ which have been selected by the some of the applications, such as Belgium, Portugal, Ireland ¹⁰⁰⁰, as briefly called out in Chapter 1. Similarly, In terms of data storage, the most privacy-preserving choice would be a decentralized and anonymized contact tracing application.¹⁰⁰¹ With a decentralized app, collected data are stored in the user's devices and are only accessed if an individual is infected.¹⁰⁰² In this regard, for instance, VenueTrace, a venue-access-based contact tracing solution summarized in ¹⁰⁰³, prioritizes user privacy through several design elements: (i) it traces venue-to-user contacts rather than user-to-user; (ii) eliminates information exchange between users; and (iii) guarantees no exposure of private data to backend servers while still enabling proximity contact tracing.¹⁰⁰⁴ They provided an efficient example of

⁹⁹⁷ Cavoukian, Ann, and Jonas, Jeff (2012). "Privacy by design ...", *op.cit.*, p.8.

⁹⁹⁸ Article 5-1-e of the GDPR, storage limitation.

⁹⁹⁹ Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha. (2020) "A survey of COVID-19 ...", *op.cit.*, p.134584.

¹⁰⁰⁰ See Stay Away App, GitHub Security Policy stayawayinesctec/stayaway-app, Security, HSE privacy policy, *op.cit.*, research section, CoronaWarn app, privacy notice, *op.cit.*, Coronaalert privacy notice, *op.cit.* section 1.

¹⁰⁰¹ See Kaya, Emre Kursat (2020) "Safety and Privacy in the Time of COVID-19: Contact Tracing Applications", Centre For Economics and Foreign Policy Studies, Cyber Governance and Digital Democracy 2020/05/EN, pp.1-11, p.8.

¹⁰⁰² *Ibid.*

¹⁰⁰³ For the full article see Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth and Ranasinghe, Damith C. (2020) "VenueTrace: a privacy-by-design COVID-19 digital contact tracing solution", Proceedings of the 18th Conference on Embedded Networked Sensor Systems, pp. 790-791, p.790.

¹⁰⁰⁴ Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth and Ranasinghe, Damith C. (2020) "VenueTrace: a privacy-by-design...", *op. cit.*, p.790.

designing the application from the beginning as per privacy considerations.¹⁰⁰⁵ Or, differently, Reichert and colleagues provided an efficient approach to contact tracing applications to provide a solution on how to make centralized contact tracing based on GPS data more privacy-preserving for users.¹⁰⁰⁶ As per their research, their main contribution lies in the application of Secure Multiparty Computation (MPC) on the real-world problem of centralized contact tracing. Using MPC on the one hand results in significantly longer runtimes when compared to other centralized approaches.¹⁰⁰⁷ On the other hand, it provides real semi-honest security, while a majority of centralized schemes rely on a trusted server and upload user data to the server for risk evaluation.¹⁰⁰⁸ For example, diversified designs are currently employed in relation to strategies for identifying contacts, the sort of notifications which are obtained, and the use of centralized versus decentralized approaches. In this regard, from data protection law perspective, we believe that blockchain as an open and shared database over which no single party has control, and transactions, which including messages exchanged when two devices come into close contact, are safely recorded in blocks.¹⁰⁰⁹ Due to the fact that blockchain does not rely on a centralized server, this can enable global access to information while simultaneously being more resistant to harmful attacks.¹⁰¹⁰ The reason is the information in each block is available to all users and cannot be tampered with, blockchain can also improve data integrity and security, lowering the dangers of impersonation or manipulating test findings or close connections. To be more specific, blockchain is unaffected since it

¹⁰⁰⁵ Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth and Ranasinghe, Damith C. (2020) "VenueTrace: a privacy-by-design...", *op. cit.*, p.790.

¹⁰⁰⁶ Reichert, Leonie; Brack, Samuel and Scheuermann, Björn (2020)."Privacy-preserving contact tracing of COVID-19 patients", *Cryptology ePrint Archive*, pp.1-2, p.1.

¹⁰⁰⁷ Reichert, Leonie; Brack, Samuel and Scheuermann, Björn (2020)."Privacy-preserving contact...", *op.cit*, p. 2.

¹⁰⁰⁸ *Ibid.*

¹⁰⁰⁹ Klaine, Paulo Valente, Zhang, Lei; Zhou, Bingpeng; Su, Yao; Xu, Hao and Imran, Muhammad (2020) "Privacy preserving...", *op. cit.*, p.60.

¹⁰¹⁰ *Ibid.*

has the potential to bridge these gaps and create a distributed environment for tracing players.¹⁰¹¹ The composure of the blockchain method is, therefore less subject to de-anonymization risks due to its complex structure, which brings a tailor-made solution for the de-anonymization or re-identification of personal data risk indicated in Chapter 2, which are the main concerns of the architectural design of the contact tracing applications. Hence, in line with the European regulatory approach, the adaptation of blockchain technology into contact tracing applications could be achieved by a solid design of the applications by taking the potential risks into consideration, as blockchain is now being used in keeping health records of patients in preserving their overall medical history without any involvement of service providers.¹⁰¹²

We, therefore, find the proposed blockchain solution¹⁰¹³ are effective and in line with the spirit of the GDPR and ePrivacy Directive, in which they proposed a Blockchain-based framework that preserves patients' anonymity while tracing their contacts using a smartphone application to interact with the proposed blockchain framework for contact tracking using Bluetooth.¹⁰¹⁴ On the top of that, it is also significantly contributing to the storage limitation perspective of the GDPR,¹⁰¹⁵ and thus from the regulatory compliance perspective, it has the approval of our research, as the blockchain method is

¹⁰¹¹ For the full decision see the European Commission Website, Danish Data Protection Agency Proposes 12 DKK Million Fine https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en (accessed on 23 June 2024).

¹⁰¹² Aslam, Bakhtawar, Javed, Abdul Rehman; Chakraborty, Chinmay; Nebhen, Jamel; Raqib, Saira and Rizwan, Muhammad (2021) "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic." *Personal and ubiquitous computing*, 22, pp.1-17, p.6.

¹⁰¹³ Author refers to Klaine, Paulo Valente, Zhang, Lei; Zhou, Bingpeng; Su, Yao;, Xu, Hao and Imran, Muhammad, respectively.

¹⁰¹⁴ For further information and details of their proposed framework see Aslam, Bakhtawar, Javed, Abdul Rehman; Chakraborty, Chinmay; Nebhen, Jamel; Raqib, Saira and Rizwan, Muhammad (2021), "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic." *Personal and ubiquitous computing*, 22, pp. 1-17.

¹⁰¹⁵ Article 5-1-e of the GDPR, storage limitation.

actually helpful for the technologies of Internet of Medical Things and cloud computing, in addition above mentioned health records.¹⁰¹⁶

Additionally, in terms of enhancing the safeguards pertaining to accuracy, confidentiality, and integrity of personal data collected by data subjects, which are other significant aspects that were partially addressed in security of processing section, and stipulated under the article 32 of the GDPR,¹⁰¹⁷ privacy by design is again of vast significance for contact tracing applications. For instance, the use of differential privacy, as briefly discussed in Chapter 3, is a method for analysing data that adds random noise to protect individual privacy. The goal of differential privacy is to enable useful data analysis while limiting the ability to infer individual-level information from the data. In the context of contact tracing apps, differential privacy might be utilized to protect the privacy of individuals while still allowing for useful data analysis. This is achieved by adding random noise to the data collected by the app, such as the proximity data used to determine exposure to COVID-19. The amount of noise added can be adjusted to balance privacy protection with the accuracy of the data analysis. To be more specific, the Safe Paths app, which was developed by researchers at MIT, allows users to share their location data with public health authorities for contact tracing purposes, but it uses differential privacy to add random noise to the data, protecting user privacy.¹⁰¹⁸ Similarly, privacy-preserving data obfuscation refers to a set of techniques that allow organizations to obfuscate or mask sensitive data in order to protect individual privacy. The answer of why such approach is required could be find the sense that could be explained with GDPR compliance standard.¹⁰¹⁹ Data encryption does not meet the high compliance

¹⁰¹⁶ Aslam, Bakhtawar, Javed, Abdul Rehman; Chakraborty, Chinmay; Nebhen, Jamel; Raqib, Saira and Rizwan, Muhammad (2020) "Blockchain and ANFIS...", *op. cit.*, p.6.

¹⁰¹⁷ Article 32 of the GDPR, security of processing.

¹⁰¹⁸ Safe Paths Application Website <https://safepaths.mit.edu/> (accessed on 11 February 2023).

¹⁰¹⁹ Kesarwani, Manish, Akshar Kaul, Stefano Braghin, Naoise Holohan, and Spiros Antonatos (2021) "Secure k-anonymization over encrypted databases", *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, pp. 20-30, p.24.

standards, since all the data encryption schemes are reversible.¹⁰²⁰ To this end, a popular approach for data anonymization, i.e., k-anonymity¹⁰²¹ could come into play with the spirit of the GDPR. k-Anonymity is a technique that ensures that each record in a dataset cannot be linked to fewer than k individuals. This is typically achieved by grouping individuals into categories based on common attributes and then modifying or suppressing data within each category to ensure that no individual can be identified. For example, a hospital might use k-Anonymity to de-identify patient data in a medical record dataset, so that researchers can analyse the data without revealing sensitive information about individual patients. With k-anonymity an original data set containing personal health information can be transformed so that it is difficult for an intruder to determine the identity of the individuals in that data set.¹⁰²² We believe that it also fits the purpose of article 9 of the GDPR, with regards to preserving sensitive personal data of data subjects, as health data could be deemed as the most sensitive special category of personal data.

Accordingly, Perera and colleagues¹⁰²³, where presented a set of guidelines, as the core of a conceptual framework, that incorporates privacy-by-design principles to guide software engineers in the systematic assessment of the privacy capabilities of Internet of Things applications and platforms, to demonstrate how their framework can be used to assess two open sources IoT platforms namely, Eclipse Smart Home and OpenIoT,¹⁰²⁴ could be a standpoint for the data protection authorities as well as the non-profit cyber security institutions to publish such guidance for each case scenario. The

¹⁰²⁰ Kesarwani, Manish, Akshar Kaul, Stefano Braghin, Naoise Holohan, and Spiros Antonatos (2021) "Secure k-anonymization...", *op.cit.*, p.24.

¹⁰²¹ El Emam, Khaled, and Dankar, Fida Kamal (2008) "Protecting privacy using k-anonymity." *Journal of the American Medical Informatics Association*, vol.15, no. 5, pp.627-637, p.628.

¹⁰²² *Ibid.*

¹⁰²³ See Perera, Charith; McCormick, Ciaran; Bandara, Arosha K.; Price, Blaine A. and Nuseibeh, Bashar (2016) "Privacy-by-design framework for assessing internet of things applications and platforms", *Proceedings of the 6th International Conference on the Internet of Things*, pp. 83-92.

¹⁰²⁴ Perera, Charith; McCormick, Ciaran; Bandara, Arosha K.; Price, Blaine A. and Nuseibeh, Bashar (2016) "Privacy-by-design framework ...", *op.cit.*, p.90.

reason is the design of contact tracing apps is quite complex and involves many experts and IT developers. For instance, when GAEN API was created as open source, as mentioned in Chapter 1, numerous countries assigned the responsibility of app development to private tech firms within their borders or to public tech entities operating within bureaucratic structures.¹⁰²⁵ For instance, countries such as Belgium, Slovenia, and Hungary adopted pre-existing European contact tracing app code.¹⁰²⁶ To be more precise, Belgium, Cyprus, and Slovenia integrated parts or the entirety of Germany's Corona-Warn-App (CWA) into their systems, while Hungary's app was constructed using an IT solution previously implemented in North Macedonia.¹⁰²⁷ Also, to be more specific on its reflection on privacy-by-design, for the creation of the Estonian HOIA contact tracing application¹⁰²⁸, more than a dozen companies and organizations took part.¹⁰²⁹ Health and Welfare Information Systems Center (TEHIK), supplies customer support for HOIA and is in charge of administering and hosting the application as well. Tartu-based Mooncascade and FOB Solutions in Tallinn also provided a contribution to the development of mobile applications, whereas Velvet, was in charge of branding the application and homepage development. Bytelogics and Fujitsu assisted in application adoption areas, whereas the company ASA Quality Services provided test assistance to HOIA, and Heisi IT developed the patient portal thereof.¹⁰³⁰ Cybernetica, Tallinn-based company whose specialization is designing secure data systems, was in charge of security architecture and analysis, in collaboration

¹⁰²⁵ June Park (2021) "Governing a Pandemic with Data...", *op.cit.*, p.86.

¹⁰²⁶ European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.32.

¹⁰²⁷ European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.32..

¹⁰²⁸See HOIA Phone Application Privacy Policy, *op.cit.*, Section 9, 10, 13, 15,

¹⁰²⁹ See E-Estonia Website, Coronavirus app HOIA the product of a unique private public partnership <https://e-estonia.com/estonias-coronavirus-app-hoia-the-product-of-a-unique-private-public-partnership/> (accessed on 23 June 2024).

¹⁰³⁰ *Ibid.*

with Guardtime, which provides blockchain-based products.¹⁰³¹ In short, considering that many expert firms were involved in the design process of European contact tracing applications, not limited to Estonian contact tracing applications, twenty four out of twenty seven total, as per the EU Commission data.¹⁰³²

However, in response to the augmented amount of third party involvement to the privacy-by-design process, there is a hybrid approach, which could be leveraged in the future, offers centralized systems suffer from the risk that people could be deanonymized from their Bluetooth broadcasts and could also reveal some of their contact if they meet a person who could contaminate them.¹⁰³³ It does reveal some part of the social graph to the determined server. Conversely, decentralized systems make public the Bluetooth broadcast of diagnosed people, which could lead to mass surveillance.¹⁰³⁴ Vaudenay argued that the debate between centralized and decentralized systems has been heavily biased. And added that none of those systems offer any decent level of privacy protection. Similarly, Shubina and colleagues are also supportive of hybrid approaches by arguing that a promising avenue for further research involves exploring various proximity-detection methods beyond BLE, including Wi-Fi, UWB, or hybrid approaches. Investigating these techniques could enhance coverage and improve the effectiveness of digital contact tracing.¹⁰³⁵

From our point of view even though the latter is related to the technical aspect of contact tracing, some hybrid directions exist and are promising. However, there is not one single approach for the designation of contact tracing applications from the scratch. The positive side is that based on their

¹⁰³¹ *Ibid.*

¹⁰³² European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices...”, *op.cit.*, p.32.

¹⁰³³ Vaudenay, Serge (2020) "Centralized or decentralized?", *op.cit.*, p.29.

¹⁰³⁴ Vaudenay, Serge (2020) "Centralized or decentralized?", *op.cit.*, p.29..

¹⁰³⁵ Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2020) "Effectiveness modelling... ", *op. cit.*, p.879.

demonstration of compliance activities as per their privacy statements, the design of the contact tracing applications employed within the GDPR jurisdictions is complying with these requirements. However, the hybrid approach still could be an efficient solution to mitigate the defective lack points of each approach. In order to establish a single contact tracing, a task force should be formed and merely devoted to the technical and organizational aspects of contact tracing applications as advised in security of processing as well. Such an initiative could play an important role in drafting an hybrid approach which could be accepted in a wider sense. There are for sure limitations to privacy by design approach, in case the purpose of the system is to do intrusive surveillance of populations, tagging a privacy-by-design label on these systems, regardless of the amount of data minimization, is misleading.¹⁰³⁶ As such, we are of the view that, as supported by the research of the author, privacy by design is not sufficient by itself in case it is only used for the implement a safer appearance for processing activities. In other words, when there is a high-risk processing activity, such as contact tracing or surveillance, the design of an architecture fulfilling each privacy requirement is not the end of the story: as an architecture is created, by definition, at a satisfactorily high level of abstraction, the remaining task is to establish appropriate mechanisms to implement it.¹⁰³⁷ The reason is, one of the repercussions of engineering privacy by design, and thus data minimization is to refrain from the processing of vast amounts of data that can later be repurposed.¹⁰³⁸ Hence, we advise data controllers to have a holistic view of each component of Privacy by design, as detailed in the DPIA-related section.

In conclusion, the privacy-by-design method is being widely used by the data controllers of contact tracing applications based on their privacy policies, and

¹⁰³⁶ Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2020) "Effectiveness modelling...", *op. cit.*, p.879.

¹⁰³⁷ Antignac, Thibaud, and Le Métayer, Daniel (2014). "Privacy by Design: From Technologies to Architectures: (Position Paper)", *Privacy Technologies and Policy: Second Annual Privacy Forum*, APF 2014, Athens, Greece, May 20-21, 2014, *Proceedings 2* Springer International Publishing, pp. 1-17.

¹⁰³⁸ Gürses, Seda, Troncoso, Carmela and Diaz, Claudia (2011) "Engineering privacy by design", *Computers, Privacy & Data Protection*, vol.14, no. 3, pp.1-25, p. 23.

it helps to designate a privacy-friendly atmosphere for contact tracing applications based on our research. In addition to this, as the privacy-by-design approach is becoming more popular among data controllers of different types of mobile applications due to evolving data protection-related risks, the value of overseeing the above-mentioned requirements from the design process of contact tracing applications could be more crucial in the future. Therefore, it is vital to align the DPIA process with the designing process of the applications to consider any potential privacy and security threats as outlined above and utilize tailor-made and cutting-edge solutions for processing activities during the designing process, i.e., blockchain technology, venue-to-user contact tracing, secure multiparty computation etc. as provided above. Most of the contact tracing applications employed within the EEA were putting an effort to do that based on their privacy policies as well as terms and conditions of the use by prioritizing anonymous processing, privacy friendly architecture and auto-deletion process, as detailed in Chapter 1. However, we must also admit that non-existence of remarkable personal data breaches till our date does not mean that privacy-by-design approach of the controllers were bullet-proof. As such, there is a chance to solidify these mechanisms by applying the aforementioned methods, which are more in line with the threats of our era for any potential use of the applications, considering the short time frame they were provided to develop these applications, and novelties brought by technologies and diseases.

5. Privacy by default

Privacy-by-default method is also significant in mitigation of the risks from the source of risks delineated in the Chapter 2. Accordingly, default privacy settings has a significant role in restricting or revealing Internet service users' personally identifiable information.¹⁰³⁹ On the one hand, highly restrictive privacy settings restricts the information sharing utilities of services, whereas

¹⁰³⁹ Nakamura, Toru; Kiyomoto, Shinsaku; Welderufael B. Tesfay, and Serna, Jetzabel (2016) "Personalised privacy by default preferences-experiment and analysis", International Conference on Information Systems Security and Privacy, vol. 2, SCITEPRESS, pp. 53-62, p.53.

on the other hand less constrained privacy settings could notably harm the privacy of users.¹⁰⁴⁰ Therefore, the term of privacy by default is also going hand in hand with the notions of purpose limitation, data minimization as well as technical and administrative sets of measures taken by undertakings with operational considerations of the apps as well. To be more specific, by default, companies/organizations ought to provide the fact that personal data at stake is processed with the ultimate privacy security, which means, for example, only processing the necessary data, keeping storage periods short, and restricting access, and so as to ensure personal data is not accessible to an indefinite number of people by default.¹⁰⁴¹ Therefore, as stated by Bygrave, the obligation includes ensuring the automatic application of specific data protection principles and default restrictions on data accessibility.¹⁰⁴² From this perspective, as it has already been highlighted in a few sections of the thesis that majority of the controllers, i.e., Germany, Netherlands, Denmark, Cyprus, Spain as well as Latvia¹⁰⁴³ and many others selected certain period of time for storage of identifiers, and by-default majority of the controllers such as, Latvia, Lithuania, Slovenia,¹⁰⁴⁴ and etc. processed with pseudonyms identifiers, or, Belgium Estonia, France¹⁰⁴⁵ and etc. relied on anonymous processing for certain type of purposes of the app. Nonetheless, considering the risks associated with Bluetooth processing, and other advanced re-

¹⁰⁴⁰ *Ibid.*

¹⁰⁴¹ See the European Commission article, What does data protection by design and default mean? available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (accessed on 15 August 2022).

¹⁰⁴² Bygrave, Lee (2017) "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements", Oslo Law Review, vol. 1, 105-120. 10.18261/issn.2387-3299-2017-02-03, p.106.

¹⁰⁴³ See Smittestopp Processing of Personal Data, op.cit., section 5., Corona Warn privacy notice op.cit, section 3-e, Coronamelder privacy policy, op.cit. section 7, Apturi Covid privacy policy, op.cit, section 7. Radar Covid privacy policy, op.cit. section 3.

¹⁰⁴⁴ See Coronaalert privacy policy, op.cit. section 3., 'Korona Stop LT' Privacy Policy op.cit section 5.2., OstaniZdrav privacy policy, op.cit, section 3., CovTracer EN Privacy notice, op.cit., section 8, when will be data deleted?

¹⁰⁴⁵ See Coronaalert privacy policy, op.cit. section 3. Tous Anti Covid, privacy policy, op.cit, section "exercising your rights", HOIA mobile application, op.cit., section "how does the app work"

identification methods of anonymised data elaborated in Chapter 2, we believe that there is automatically room for adjustment on the term of “by-default”, in light of the needs of contact tracing era.

More specifically, the ideal scenario is to have a customized privacy and utility ideal preference setting that is tailored to the user's specific requirements.¹⁰⁴⁶ The problem is that network operators do not provide privacy-optimal and personalized preference settings by standard, and most users are unable to generate such settings on their own. Eventually, end users' privacy worries are considerably increased when their privacy choices are not correctly and appropriately configured. As also detailed in security of processing section, given that the EDPB strongly emphasizes the critical role of smart cryptographic methods for securing data in servers and applications, especially for exchanges between applications and remote servers. This includes ensuring proper authorization, such as through mutual authentication between the application and server or the requirement for reporting by users. An example highlighted was the use of single-use codes tied to a pseudonymous identity of an infected person and associated with a testing station¹⁰⁴⁷, it is fair to notice that the significance of data protection by design is also underlined. In other words, these applications should be designed from the scratch by considering such elements of the GDPR by default. Therefore, each citizen using contact tracing applications will have to apply it for these applications, not less than the rights of the data subject regulated between article 12 and 23 of the GDPR.¹⁰⁴⁸ With regards to the use of these rights, the value of the online interface has increased enormously. The interface of applications should make these defined rights available to the data subject, at least it should be expressed in a policy like the website policies provided by other banks, social media companies, insurance companies, and the contact person for the enforcement of the rights should be shown, and by default must

¹⁰⁴⁶ Nakamura, Toru; Kiyomoto, Shinsaku; Welderufael B. Tesfay, and Serna, Jetzabel (2016) "Personalised Privacy by Default Preferences", *op. cit.*, p.53.

¹⁰⁴⁷ Guideline 04/20, *op.cit.*, p.9.

¹⁰⁴⁸ Article 12 to 23 of the GDPR, Data Subject Rights.

be reiterated that the use of these applications is normally voluntary and is considered as support to control the spread of the virus.¹⁰⁴⁹

Having mention this generic but important considerations, it is important to pinpoint how these rights under the GDPR, by default protected. We believe it can be done in countless ways. For example, the users' privacy can be preserved using varied mechanisms, e.g., data anonymization, differential privacy, and decentralized app development,¹⁰⁵⁰ as also delineated in the previous section. Nevertheless, it is determined that anonymization systems are not providing efficient privacy preservation and decentralized application development is still at the initial stage and developing at a slow pace. On top of that, anonymization of data by default will not solve any problem described in Chapter 2 by itself. This anonymization should be in harmony with efficient configurable settings and opt-in, opt-out functions. Nevertheless, there is no common answer in the World as to when configurable settings should be used and when wired-in functionality without an option to adapt should be preferred.¹⁰⁵¹ Wired-in functionality may be regarded over-protective or even invasive for the autonomy and informational self-determination of the individual, both important core values of privacy protection.¹⁰⁵² Accordingly, a lot of websites, mobile phones, mobile applications and other devices and programs which can facilitate or inhibit tracking are pre-selected to enable tracking today, as such "Track-Me" is a quasi-default.¹⁰⁵³ These settings are not full-fledged defaults, in that opting-out is not always feasible, some devices and programs could not be used without tracking allowed and some

¹⁰⁴⁹ Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital contact tracing applications and techniques... ", *op.cit.*, p.4.

¹⁰⁵⁰ Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital...." *op.cit.*, p.100072.

¹⁰⁵¹ Hansen, Marit (2013), "Data protection by default in identity-related applications", *IFIP Working Conference on Policies and Research in Identity Management*, Springer, Berlin, Heidelberg, pp.4-17, p.7.

¹⁰⁵² *Ibid.*

¹⁰⁵³ Willis, Lauren E. (2014) "Why not privacy by default." *Berkeley Tech. LJ.*, vol.29, pp.61-134, p.66.

trackers track consumers even during program or device settings are in the Do-Not-Track selection.¹⁰⁵⁴ In case configurable settings are selected, their granularity must be determined, on the one hand, fine-grained controls may be more appropriate to reflect any situation, on the other hand, they might be too complex for users to understand their meaning and the impact of modification.¹⁰⁵⁵ This could end up as an increase in the unwanted consequences while changing the settings. Considering the discussions, it is plausible to state that organizations and developers that create applications must decide on a default privacy configuration that may or may not account for user privacy needs and desires.¹⁰⁵⁶

While scrutinizing the right defaults, two different types of configurations ought to be distinguished:¹⁰⁵⁷

- The setting of an additional process that is not strictly required for the application's original functionality or simple use. This is typically accompanied with a new purpose (e.g., an extra newsletter subscription or additional data transmission to third parties who evaluate the data). This additional process may or may not be seen as useful by the data subject.
- The configuration of a procedure needed for the proper within the application- this is where the default value is chosen. For example, if certain data must be transferred, it may or may not be encrypted by default. Another example is how the irrefutable payment process for certain products or services is handled, for as through prepaid, credit card, or direct debit.

¹⁰⁵⁴ *Ibid.*

¹⁰⁵⁵ Hansen, Marit (2013), "Data protection by default in identity-related applications", *op. cit.*, p.7.

¹⁰⁵⁶ Watson, Jason; Richter Lipford, Heather and Besmer, Andrew (2015) "Mapping user preference to privacy default settings", *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol.22, n. 6, pp. 1-20, p.3.

¹⁰⁵⁷ Hansen, Marit (2013), "Data protection by default in identity-related applications...", *op. cit.*, p.7.

Nevertheless, what is more interesting could be derived from the study of Wang, and colleagues, in which participants perceived a potential violation of their privacy, so they tended to opt-out of the app altogether instead of changing their default privacy settings.¹⁰⁵⁸ Collectively, their findings suggest that app developers should carefully consider the relevancy of the information they tend to request in the process of designing privacy notices. When requesting information out of context, app developers could harm their reputations and drive away potential users.¹⁰⁵⁹ Also, considering that secure processing requires the secure collection, processing, storage, and discarding of contact tracing information of people in real-time, without impinging on their privacy and rights.¹⁰⁶⁰ Therefore, in order to reach a meaningful number, the applications need to gain trust and usefulness to its users,¹⁰⁶¹ as elaborated in Chapter 1 and Chapter 3. As for the reflection of the topic to the contact tracing applications, from our point of view, data controllers could be better off by using it, and it has to be determined how the default setting should be as clear as possible, so that data subject citizens can have full control of their personal data processed by the application without any doubt.

That said, main challenges are concerning to the technical, usability, and privacy matters or necessities reported by some users.¹⁰⁶² This means that most tracing apps were not publicly well-received and had low penetration levels, which hinders their effectiveness.¹⁰⁶³ Correspondingly, behavioural

¹⁰⁵⁸ Wang, Na; Wisniewski, Pamela; Xu, Heng and Grossklags (2014) "Designing the default privacy settings for Facebook applications", *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing*, pp. 249-252, p.252.

¹⁰⁵⁹ Wang, Na; Wisniewski, Pamela; Xu, Heng and Grossklags (2014) "Designing the default privacy settings ...", *op.cit.*, p.252.

¹⁰⁶⁰ Elkhodr M, Mubin O, Iftikhar Z, Masood M, Alsinglawi B, Shahid S, Alnajjar (2021) " F Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search anContent Analysis", *J Med Internet Res.*, vol.23, n.2, e23467, pp.1-17, p.14.

¹⁰⁶¹ See Kaya, Emre Kursat (2020) "Safety and Privacy in the Time of COVID-19...",*op.cit.*, p.7.

¹⁰⁶² *Ibid.*

¹⁰⁶³ Elkhodr M, Mubin O, Iftikhar Z, Masood M, Alsinglawi B, Shahid S, Alnajjar F (2021) "Technology, Privacy, and User Opinions...", *op. cit.*, p.14.

studies indicated that default rules tend to ‘stick’ due to certain reasons.¹⁰⁶⁴ For instance, the individuals may ignore the default rules (being idle), have no strong preference, or not have sufficient knowledge to decide. It might also be the case that concerned individuals regard default rules as suggestions or recommendations from policymakers, regulators, or service providers, who have acted as choice architects in that case.¹⁰⁶⁵ On the other hand, active choosing may provide more freedom to the individual who must make a choice, as there is no default rule, that might influence or even determine the choice. In addition, the obligation for active choosing, may, in principle, force the individual to educate himself before making the choice.

Therefore, our evaluation on the privacy-by-default approach of contact tracing applications is that to achieve this goal, employing the default option of contact tracing application for as most privacy preserving technique, it is even possible that the burden of proof for compliance with the GDPR could be reduced to some extent. Once the contact tracing applications start to process personal data of the users with a default option that sets forth the most privacy friendly option for the processing at stake, this could lead to solidified compliance mechanism. At the same time, it is efficient for data subjects too, as they can feel the assurance provided by the application itself that most privacy friendly option is utilized by the applications. This situation may not only increase the amount of trust between data controller and data subjects, but at the same time may higher the amount of the use of contact tracing applications. The underlying reason thereof is that one of the biggest concerns at stake pertaining to the intrusiveness of contact tracing applications could be diminished in a manner that is in line with the GDPR principles.¹⁰⁶⁶ Moreover, from a user experience standpoint, the applications would be easier to use. Privacy-friendly default settings generally ensure

¹⁰⁶⁴ Jasmontaite, Lina; Kamara, Irene; Zafir-Fortuna, Gabriela and Leucci, Stefano (2018) "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", *Eur. Data Prot. L. Rev.*, vol. 4, pp.168- 189, p.184.

¹⁰⁶⁵ Jasmontaite, Lina; Kamara, Irene; Zafir-Fortuna, Gabriela and Leucci, Stefano (2018) "Data protection by design and by default...", op.cit., p.184.

¹⁰⁶⁶ Article 5 of the GDPR, principles relating to processing of personal data.

maximum privacy, eliminating the need for users to modify settings upon first use to protect their data.¹⁰⁶⁷ Should users wish to change these settings, they must opt-in and adjust them manually, such as choosing to share more of their personal data with others.¹⁰⁶⁸ Also, we are of view that such dashboards wherein data subjects can opt-in or change the settings of processing, should be extremely clear and user-friendly for making it feasible for everyone. Therefore, even the trust gained by such default implementation is of massive significance to user experience and public health. What we called out in consent section for allowing different type of processing activities by user consent would be a great example of this. However, as discussed, not all the controllers implemented this approach.

In addition to this, we would like to pinpoint further cutting-edge approaches in line with the GDPR, rather than enumerating GDPR principles and their default application all over again. To this end, what is not mentioned in the relevant literature is that the logic behind the federated social media platforms could be used as a starting point for contact tracing applications within the scope of privacy by default approach.¹⁰⁶⁹ To briefly provide a background, the Fediverse is a group of federated social media platforms and related assisting servers, separated from each other, which are interoperable and thus allow their users to interact across different platforms. For this, The Fediverse relies on open protocols which grant platforms a common language to communicate with other platforms and exchange profile data, private messages, contributions to the public timeline, etc.¹⁰⁷⁰ Therefore, interact with other users can choose to sign up on any interoperable Fediverse platform and still who have executed the same. One such open protocol for social media interoperability is the W3C ActivityPub. An alternative to centralized,

¹⁰⁶⁷ Calzolaio, Simone (2016) "Digital (and privacy) by default...", *op.cit.*, p.185.

¹⁰⁶⁸ Calzolaio, Simone (2016) "Digital (and privacy) by default...", *op.cit.*, p.185.

¹⁰⁶⁹ See EDPS (2022) Tech Dispatch Federated Social Media Platforms https://edps.europa.eu/system/files/2022-07/22-07-26_techdispatch-1-2022-federated-social-media-platforms_en.pdf (accessed on 15 September 2022,), p.1.

¹⁰⁷⁰ EDPS (2022) Tech Dispatch Federated Social Media Platforms, *op.cit.*, p.1.

incompatible social media platforms is provided by the Fediverse.¹⁰⁷¹ Additionally, the Fediverse's users are dispersed across a number of platforms. Less user data is at risk if one of those platforms experiences a data breach than on centralized social media. Additionally, this reduces the motivation for malicious attacks. Utilizing open-source software enables public reviews of and an honest discussion about how such platforms handle data.¹⁰⁷² The underlying open protocol of federated platforms, which are widely mentioned these days, such as W3C ActivityPub, also has a need to implement data protection by design and default, as the outcome of a mutual endeavour. As a fundamental component of such federated platforms, the protocol supplies assistance to bundle developments, yet it could slow down advancements where any conflict appears.

What we would like to point out is the perspective brought by Fediverse application seem to be useful for contact tracing applications in a way that emphasizes the implementation of privacy by design and privacy by default principles with full transparency and open protocol strictly devoted to the apps, as also mentioned under the notice section, which can help to bundle developments. In other words, distributed social networks represent a model that can plausibly return control and choice to the hands of the user¹⁰⁷³, which is exactly what we are looking for in contact tracing applications by default as well. Furthermore, although it is not identical, another privacy-by-default technique in line with the GDPR considerations would be Federated learning, which employs a comparable approach, involving machine learning to educate an algorithm across various decentralized devices without transmitting or exchanging the data from these devices. This data remains locally stored, ensuring higher levels of privacy compliance. This method stands apart from centralized machine-learning systems, where all data gets

¹⁰⁷¹ EDPS (2022) Tech Dispatch Federated Social Media Platforms, *op.cit.*, p.3.

¹⁰⁷² EDPS (2022) Tech Dispatch Federated Social Media Platforms, *op.cit.*, p.3.

¹⁰⁷³ Esguera, Richard (2011) "An Introduction to the Federated Social Network," EFF, available at: <https://www.eff.org/deeplinks/2011/03/introduction-distributed-social-network> (accessed on 22 June 2024).

uploaded to a single server.¹⁰⁷⁴ It differs from other centralized machine-learning systems where all data is uploaded to one server., is used to protect the privacy of individual users by allowing their data to be used for model training without being shared with other parties within the scope of contact tracing apps. One example of a contact tracing app that uses federated learning is the PACT app, which was developed by researchers at the University of Washington.¹⁰⁷⁵ The PACT app uses Bluetooth technology to detect when two users are in close proximity and stores encrypted proximity data on each user's device. The app uses federated learning to train a machine learning model on the encrypted data, allowing for effective contact tracing without sharing users' raw data. The global model is then deployed to each device, allowing for local predictions to be made without revealing the raw data. Identically, another example of a contact tracing app that uses federated learning is the Co-Epi app, which was developed by researchers at Harvard University.¹⁰⁷⁶ The Co-Epi app uses Bluetooth technology to detect when two users are in close proximity and stores encrypted proximity data on each user's device. The app uses federated learning to train a machine learning model on the encrypted data, allowing for effective contact tracing without sharing users' raw data. The global model is then deployed to each device, allowing for local predictions to be made without revealing the raw data. Thus, federated learning is an attractive solution for multiple application domains and technologies, from medical applications to the Internet of Things, and is subject to intensive research.¹⁰⁷⁷

Additionally, as further reflection of the federated platforms into contact tracing app could be found in the sense that depending on open protocols that grant platforms a common language to swap profile data, personal messages,

¹⁰⁷⁴ Digiday Website, What is Federated Learning? <https://digiday.com/media/what-is-federated-learning/> (accessed on 22 February 2023).

¹⁰⁷⁵ PACT Application Website <https://pact.cs.washington.edu/> (accessed on 22 February 2023).

¹⁰⁷⁶ COEPI Application Website <https://coepi.org/> (accessed on 22 February 2023).

¹⁰⁷⁷ Gosselin, Rémi; Vieu, Loïc; Loukil, Faiza and Benoit, Alexandre. (2022) "Privacy and Security in Federated Learning: A Survey", *Applied Sciences*, vol.12, no. 19, 9901, pp.1-15, p.2.

public timeline contributions, etc. with other contact tracing applications, which approach may have effectively validated a unified data collection, processing, and transfer regime exclusively applicable to COVID-19 contact tracing apps as an exception to national privacy regulations, as proposed by the study of Du, Raposo, and Wang.¹⁰⁷⁸ This is also in line with the recommendation presented in the transparency and data minimization sections for the standardized approach of contact tracing applications. However, regardless, in light of the above-mentioned discussions, the most fundamental requirement is to apply by default, the data minimization, purpose limitation, retention and secure processing matters must be implemented by contact tracing applications under the GDPR, as reiterated by the Commission¹⁰⁷⁹, to proceed even a step further, these practices would be harmonized with the cutting-edge methodologies in line with the spirit of the GDPR, as detailed above, i.e. federated platforms, configurable settings and etc. by considering the public interest and the privacy of people. As a supportive view to our perspective, Opinion 6/2020 on a proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation could be simplified¹⁰⁸⁰ In the named decision, as the EDPS set out that tax compliance is an important objective of public interest, yet The pursuit of such an objective and the preservation of individuals' privacy and personal information should coexist in harmony.¹⁰⁸¹ In this regard, he emphasized the crucial need to prioritize the integration of data protection principles such as designing systems with privacy in mind, default settings that prioritize data minimization, and ensuring data accuracy, which is especially pertinent in the

¹⁰⁷⁸ Du, Li; Raposo, Vera Lúcia and Wang, Meng (2020) " COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the Gap for International Pandemic Control" JMIR Mhealth Uhealth;8(11):e23194 doi: [10.2196/23194](https://doi.org/10.2196/23194) PMID: [33156804](https://pubmed.ncbi.nlm.nih.gov/33156804/) PMCID: [7704120](https://pubmed.ncbi.nlm.nih.gov/7704120/) , pp.1-10, p.6.

¹⁰⁷⁹ See Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).

¹⁰⁸⁰ See EDPS Opinion on the proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation available at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-council-directive_en (accessed on 23 June 2024).

¹⁰⁸¹ *Ibid.*

context of automated information exchanges among national tax authorities.¹⁰⁸² Our perspective on the topic that the same logic can be applied to contact tracing applications as well, given that regulatory concerns are relatable. Considering that contact tracing is also significant objective of public interest, the balance ought to be struck between the achievement of such goal and the right to privacy and personal data protection by implementing principles of data protection by design and by default, data minimization and data accuracy in the context of processing activities of contact tracing applications and personal data exchange between the applications.

Therefore, in conclusion, privacy-first approach was taken by the contact tracing applications utilized within the GDPR jurisdictions by using voluntary applications, limited storage period and anonymization of the data collected, as indicated above. We believe that these practices could be enhanced considering the outcomes of the frequent DPIA as in line with the DPIA requirements section, and supported by the solutions we discovered above. However, we would like to reiterate that there is always a chance to discover more privacy-friendly features to the existing applications as default, due to constantly evolving nature of the data science and cyber security threats. Non-existence of remarkable personal data breaches should not mislead controllers for the success of the privacy features by itself. Accordingly, as this thesis is dealing with the evolving aspects of contact tracing activities, there is always a chance to solidify these mechanisms by considering the novelties brought about by technologies and diseases.

¹⁰⁸² See EDPS Opinion on the proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation available at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-council-directive_en (accessed on 23 June 2024).

V- EUROPEAN UNION GUIDELINES AND DOCUMENTS ON CONTACT TRACING

As reiterated in the previous chapters, data protection and privacy related aspects of the contact tracing applications are not only overseen by the main data protection regulations of the EU, namely GDPR¹⁰⁸³, and e-Privacy Directive¹⁰⁸⁴, but also subject to further guidance and recommendations issued by the European Union institutions due to the specific nature of the processing activities.

The reason why such need arose in the first place is that due to broader nature of the EU regulations on data processing activities, there was a need for tailor-made guidance on pandemic-specific implementation of these regulations. In other words, given that the core data protection regulations are creating the ground layer for the data protection aspects of the applications, these guidelines have been helping to provide more detailed and focused approach on the applications' compliance activities. To this end, the EU Commission and the other EU institutions/bodies such as the European Data Protection Board¹⁰⁸⁵, the European Data Protection Supervisor¹⁰⁸⁶ drafted notable guidelines to navigate the issue of data protection management during the use of contact tracing applications. In particular, to list these guidelines and documents, we can mention that the EDPB issued Guidelines

¹⁰⁸³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter referred as 'GDPR').

¹⁰⁸⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (the "ePrivacy Directive").

¹⁰⁸⁵ The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. For further information See the EDPB Website, https://edpb.europa.eu/edpb_en (accessed on 12 May 2023).

¹⁰⁸⁶ The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority. For further information see https://edps.europa.eu/about/about-us_en (accessed on 12 May 2023).

04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.¹⁰⁸⁷ Within the same remit, the EU Commission issued a communication on Apps supporting the fight against Covid-19.¹⁰⁸⁸ Moreover, the Commission issued Commission Recommendation (Eu) 2020/518 of 8 April 2020 on a common Union toolbox.¹⁰⁸⁹ Likewise, eHealth Network¹⁰⁹⁰, in conjunction with the Commission drafted and published a detailed guideline on the applications, which was called toolbox.¹⁰⁹¹ Lastly, with regards to the governance of the data transfers and interoperable functioning of the applications, the Commission issued interoperability guideline.¹⁰⁹² Having said that, in addition to these main guidelines, the EDPB, the EDPS and the Commission did also publish certain information notes and guides such as Contact Tracing with Mobile Applications¹⁰⁹³ and Guidance of the Commission.¹⁰⁹⁴

The European Union Fundamental Rights Agency (FRA)¹⁰⁹⁵ has conducted extensive research to explore the impact of the COVID-19 pandemic on

¹⁰⁸⁷ EDPB (2020) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.

¹⁰⁸⁸ Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670 (accessed on 12 May 2023).

¹⁰⁸⁹ Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

¹⁰⁹⁰ 'eHealth Network' means the network established by Article 14 of Directive 2011/24/EU and whose tasks have been clarified by the Implementing Decision (EU) 2019/1765.

¹⁰⁹¹ eHealth Network (2020), Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States.

¹⁰⁹² eHealth Network (2020) Interoperability guidelines for approved contact tracing mobile applications in the EU.

¹⁰⁹³ EDPS (2020) TechDispatch on Contact Tracing with Mobile Applications 1, 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-05-08_techdispatch-tracing_en.pdf ((accessed on 12 May 2023).

¹⁰⁹⁴ Coronavirus: Guidance to ensure full data protection standards of apps fighting the pandemic.

¹⁰⁹⁵ FRA is an independent centre of reference and excellence for promoting and protecting human rights in the EU, for further details see <http://fra.europa.eu/en/about-fra> (accessed on 12 May 2023).

fundamental rights.¹⁰⁹⁶ Pertaining to privacy and data protection aspects of the applications, a bulletin has been published on the nuances of contact tracing apps and their processing activities. Suitably, evidence collected by the agency indicates that nearly all EU data protection authorities have issued pandemic-related guidelines. These declarations affirm that the right to health and the protection of personal data go hand in hand. It also emphasizes that any act that violates privacy or data protection rights must be lawful, necessary, and appropriate.¹⁰⁹⁷

Therefore, as seen, there have been plenty of developments regarding the guidelines of the Commission, the EDPB and other European institutions to navigate the data protection aspects of the applications. Accordingly, in this chapter of the thesis, we are going to investigate and analyse what extent data controllers comply with these guidelines and documents and provide our contribution as to whether there are certain areas of improvement from both controllers' and regulators' perspective. In each following section, we will deep dive into the respective guidelines and assess the nuances thereof and will refer to the previous chapters where needed to elaborate the analysis of the aforementioned guidelines. Also, by implementing an in-depth analysis for each guidance, it is possible to observe the consolidated approach brought by the EU authorities on data protection law. Accordingly, we are going to examine each of them from the perspective of compatibility and unity as well.

1. Guidelines 04/2020 On The Use Of Location Data And Contact Tracing Tools In The Context Of The COVID-19 Outbreak

The EDPB guideline provided drastic contribution to the implementation of the data protection necessities by data controllers as it provided elaborate guidance on many aspects of data protection requirements. To begin it with, the EDPB emphasized the importance of certain data protection principles from the beginning by setting out that when Member States or EU institutions

¹⁰⁹⁶ Kędzior, Magdalena (2021) "The right to data protection and the COVID-19 pandemic: the European approach", *ERA forum*, vol. 21, no. 4, Springer, pp. 533-543, p.539.

¹⁰⁹⁷ Kędzior, Magdalena (2021) "The right to data protection ...", *op.cit.*, p.538.

take measures involving the processing of personal data to combat COVID-19, they should follow the general principles of effectiveness, necessity and proportionality,¹⁰⁹⁸ which are reflected onto the design of the applications, as precisely documented from the beginning, whose details was provided in the previous Chapters. As pointed out earlier, such principles-based approach from the beginning is the result of unified approach created for European data protection perspective¹⁰⁹⁹, which aims to strengthen the common application of certain rules across the Europe. Accordingly, the guideline is divided into three main categories, namely;

- use of location data,
- legal analysis,
- functional analysis and recommendations and analysis guide.

Correspondingly, to start with the use of location data part, the Guideline elaborated the aspects of location data use by controllers, by referring to article 6 and 9 of the ePrivacy directive¹¹⁰⁰ as well as the GDPR article 23¹¹⁰¹. Predominantly, it emphasized the importance of using to anonymization for the processing location data. Achieving anonymization requires careful processing of location data to meet requirements of “reasonability test”. Such processing therefore involves examining location records in their entirety and, where appropriately and effectively implemented, using available robust anonymization techniques to identify data from relatively large groups of individuals.¹¹⁰²

This is in line with the discussions in chapter 4 on location data. From data controllers’ perspective, based on our review detailed in Chapter 3 and 4, the

¹⁰⁹⁸ EDPB (2020) Guidelines 04/20, *op.cit.*, p.3.

¹⁰⁹⁹ For further details on the European approach on data protection law see European Commission, Data Protection in the EU https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 15 July 2023).

¹¹⁰⁰ See Art 6 and 9 of the ePrivacy Directive.

¹¹⁰¹ See Article 23-1 of the GDPR, restrictions.

¹¹⁰² EDPB (2020) Guidelines 04/20, *op.cit.*, p.6.

approach brought by data controllers to address privacy concerns is the use of privacy-preserving contact tracing apps. They acted positively in regard to utilizing techniques like Bluetooth-based proximity detection or decentralized data storage to minimize the collection and storage of personally identifiable information. By anonymizing and encrypting data, these tools ensure that individuals' identities and locations are protected. Accordingly, data controller, in most, applied this anonymisation target as detailed in Chapter 3 within the scope of the GDPR already, which is an important indication of fulfilling the similar requirement set out under the EDPB Guideline. However, the study of Hatamian and colleagues, they discussed the potential problematic aspects brought by the EDPB Guideline¹¹⁰³ by stating that even though in some cases apps state (in their privacy policies) that even though some apps explicitly state that they need location data (in their privacy policies), this is still problematic and not in line with best privacy and security practices. This is because many apps, including Coronavirus-SUS, Ito, Covid Safe, PrivateKit, and others, failed to disclose whether they used any dangerous permissions, including location-related ones, and many of them began to access data in an opaque way¹¹⁰⁴. This does not imply that Bluetooth-using apps may actively exploit location permission, though. The purpose of granting location access is to turn on the default system configuration. Placement Services.¹¹⁰⁵ Some of these apps (Ito, Covid Safe, Coalition, etc.) claim to be based on BLE technology, but analysis shows that they were accessing location-based permissions.

From our perspective, although it is not identical due to jurisdictional differences, the application implemented in China would be a useful sample in the similar vein. In Chinese jurisdiction, mobile payment systems, including contactless money transfers and mobile wallets, are popular digital payment

¹¹⁰³ For the full study see Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021) "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps." *Empirical software engineering* 26, pp. 1-51.

¹¹⁰⁴ Hatamian, Majid, Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar "A privacy and security analysis....", *op.cit.*, p.28.

¹¹⁰⁵ *Ibid.* p.29.

apps in China.¹¹⁰⁶ These apps combine user data such as location, health, and financial data to generate a customized personal infection risk status. This is done in partnership with government agencies, which determine user access to transportation, shops, and other public spaces.¹¹⁰⁷ Such approach faced with push back from data subjects, which is compatible with the direction set out by the Guideline for the use of intrusive location data, therefore, we find it efficient to set out the boundaries thereof. To mitigate any potential concerns resulted from the intrusiveness of the processing for location data, which was detailed in the EDPB guideline, Apple and Google released a joint document¹¹⁰⁸ with the technical specifications of a Privacy-Preserving Contact Tracing API supported by their operating systems based on BLE.¹¹⁰⁹ The specification, known as Exposure Notification, aims to balance energy consumption, user privacy, and effectiveness.¹¹¹⁰ It is supposed to become the layer on which every contact tracing application may be based on.¹¹¹¹ However, still there are aforementioned concerns around BLE are existing, and from our perspective, particularly, recently, the case in Germany regarding the use of a local contact tracing applications, whose users way more limited, raised a skepticism about the location tracking in practice. To be more specific, in order to find witnesses in a case of local crime, German police used a contact tracing app.¹¹¹² Advocates for data protection were outraged by the scandal, and politicians were warning that

¹¹⁰⁶ Jalabneh, Rawan; Syed, Haniya Zehra; Pillai, Sunitha; Apu, Ehsanul Hoque; Hussein, Molla Rashied, Russell Kabir, Arafat SM Yasir; Majumder, Md Anwarul Azim; and Saxena, Shailendra K (2021) "Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: A literature review", *Applications of Artificial Intelligence in COVID-19*, pp. 389-404, p.398.

¹¹⁰⁷ *Ibid.*

¹¹⁰⁸For further details of the document refer to Apple Website, Privacy-Preserving Contact Tracing, <https://www.apple.com/covid19/contacttracing/> (accessed on 23 June 2024).

¹¹⁰⁹ Maccari, Leonardo, and Cagno, Valeria (2021) "Do we need a contact tracing app?", op.cit., p.12.

¹¹¹⁰ Maccari, Leonardo, and Cagno, Valeria (2021) "Do we need a contact tracing app?", op.cit., p.12.

¹¹¹¹ Maccari, Leonardo, and Cagno, Valeria (2021) "Do we need a contact tracing app?", op.cit., p.12.

¹¹¹² DW Website, German Police under fire for misuse of contact tracing application <https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597> (accessed on 22 June 2024).

misuse of the app could erode public confidence.¹¹¹³ Accordingly, in a statement, Mainz's public prosecutors stated that they have opened an investigation and are making sure that the pertinent data would not be used further. Additionally, there have not been any other instances that are currently known where police were able to access the app's data for an investigation. Therefore, the Guideline would have proposed a detailed response to mitigate any sort of ambiguity in the eyes of data subjects and scholars, not only limited to this case but also for any other skepticism arose. We are of the view that, as a potential solution for the benefit of data controllers as well as data subject users, this would have been achieved by detailed Q&A section, which could address each concern raised by individuals, as data controller implemented precisely in their websites.

Furthermore, with regards to the reasonability term referred, the guideline stated that "reasonability test" must consider both objective factors (such as time and technical capabilities) and contextual factors that may change from case to case (such as the rarity of an event, population density, the nature of the phenomenon, and the volume of data).¹¹¹⁴ If the data does not pass this test, it has not been anonymized and is still subject to the GDPR.¹¹¹⁵

We believe that from the regulatory perspective the boundaries of this statement is quite vague, therefore needs further guidance to provide efficient interpretation of the issue to prevent any feared events described in Chapter 2 regarding the insufficient application of anonymization of the processed personal data. To this end, the Guideline also provided the same by referring to the community of re-identification attacks.¹¹¹⁶ Accordingly, the importance of the anonymized data and pseudonyms identifiers were also delineated in

¹¹¹³ DW Website, German Police under fire for misuse of contact tracing application <https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597> (accessed on 22 June 2024).

¹¹¹⁴ EDPB (2020) Guidelines 04/20, *op.cit.*, p.5.

¹¹¹⁵ EDPB (2020) Guidelines 04/20, *op.cit.*, p.5., p.6.

¹¹¹⁶ EDPB (2020) Guidelines 04/20, *op.cit.*, p.6.

the UK counterpart of the EDPB Guideline¹¹¹⁷, i.e., ICO Contact tracing guideline, although it is dealing with the UK apps, still providing context for the European applications, given that both jurisdictions are using the GDPR. To be more clear, as per the ICO guideline, pseudonymization is an important aspect to the pseudonymous IDs used in proximity data must be updated periodically in accordance with the processing goal.¹¹¹⁸ Similarly, we observed that the same approach is also presented by the EDPS, which indicated that in order to reduce the danger of data linkage and re-identification, apps can use pseudonymous IDs for proximity contacts and update them frequently, for example every 30 minutes.¹¹¹⁹ Therefore, from our angle, each supervisory authority did their part on emphasizing the seriousness of re-identification related risks, whereas at the same time, pointing out the right direction to prevent such attacks. As further discussion point for this matter, within the same remit, the study of Bradford and colleagues referring to EDPB's anonymization criteria indicated that while Google and Apple assert that the data handled via the Exposure Notification System (ENS)¹¹²⁰ is 'anonymous,' they have implemented several measures within their design to prevent re-identification. These measures align with the GDPR's principles of data minimization and the security of processing.¹¹²¹ These controls result in data that is at least pseudonymized, For public health authority apps, these controls may render the ENS data fully anonymous. However, depending on how the apps are designed, the operating entities could collect personally identifiable information, such as IP addresses, in addition to the encrypted

¹¹¹⁷ ICO guidance COVID-19 Contact tracing: data protection expectations on app development *op.cit.* p.9.

¹¹¹⁸ ICO guidance COVID-19 Contact tracing: data protection expectations on app development *op.cit.* p.9.

¹¹¹⁹ The EDPS (2020) Tech Dispatch, Contact Tracing with Mobile Applications, Issue 1, p.3.

¹¹²⁰ For further explanation on Exposure Notification see COVID-19 Exposure Notifications: Technology Helping Public Health Agencies Fight the Pandemic, available at <https://www.google.com/covid19/exposurenotifications/> (accessed on 15 July 2023).

¹¹²¹ Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes." *Journal of Law and the Biosciences* 7, no. 1, Isaa034, pp.1-21, p.7.

diagnosis keys generated by the ENS,¹¹²² which was listed under the data protection related risks in Chapter 2 as well. As good news for data protection law, none of the controllers in the EEA acted in breach of these necessities for processing excessive location data or of implementing the due care on the pseudonymization as it was detailed in their privacy policies and technical documentation indicating their privacy-by-design approach.

With regards to the legal analysis part of the applications, the Guideline first specified and named the types of the data controllers for contact tracing processing activity, including but not limited to national health authorities or other envisaged controllers.¹¹²³ As detailed in Chapter 1 and Chapter 3, the general trend on the indication of the identity of controllers are in line with the specification provided by the EDPB. In other words, each of the controllers, both in line with the GDPR and the EDPB guideline, set out the identity of the controllers in a clear and unambiguous manner at the outset of the applications.

From our point of view, this is strong attitude on the solidification of the data controller accountabilities as well, which may have an impact on data subject rights, any potential data breach management and so forth. Therefore, we believe that both regulators and data controllers are in a good position to emphasize and implement such requests precisely. However, we note that there is an inconsistency in the language of the applicable law to the contact tracing applications. To be more concrete, the Guideline stated in one paragraph of the legal analyses part that contact tracing applications require storing and/or accessing data that has already been saved in the terminal, which is covered by Art. 5(3) of the ePrivacy Directive¹¹²⁴ with regard to the processing's legality, whereas at the same time referring that the requirement to carry out a task in the public interest, or Art. 6(1)(e) GDPR, is the most

¹¹²² Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps...", *op.cit.*, p.7,

¹¹²³ EDPB (2020) Guidelines 04/20, *op.cit.*, p.7.

¹¹²⁴ See Article 5 (3) of the ePrivacy Directive.

pertinent legal ground for the processing.¹¹²⁵ Therefore, from the EDPB perspective, it would be clearer to indicate the right direction of lawful basis for contact tracing applications' controllers. On the other hand, from controller perspective, it is pleasing to observe that they applied the lawful basis precisely and did not abuse it, as per the analysis in Chapter 3 and 4.

Subsequently, the EDPB emphasized that the legal foundation or legislative legislation that establishes the legal basis for the use of contact tracing applications should include significant precautions, such as a mention of the application's voluntary nature.¹¹²⁶ The EDPS was also supportive of voluntary nature of the applications as per their views published on the apps, by indicating that lack of explanations on how the tracing apps work and how they protect the user's privacy might create a lack of trust. Therefore, the use of tracing apps should be voluntary and transparent to the user.¹¹²⁷ Correspondingly, the EDPB indicated that along with an unambiguous identification of the controllers included, the aim and precise limitations regarding further use of the personal data should be specified.¹¹²⁸ It is important to identify the categories of data as well as the recipients and purposes for which personal data may be exposed. Additional protections should be included depending on the degree of interference, considering the type, extent, and aims of the processing. We were supportive of this perspective, as discussed in transparency part of Chapter 3, since the boundaries of the processing activity, identity of controller and limits of purpose and legal basis of processing is of massive importance for the healthy implementation of data protection compliance activities, in line with the Guideline as well as the GDPR¹¹²⁹ and ePrivacy Directive¹¹³⁰. Although this is

¹¹²⁵ EDPB (2020) Guidelines 04/20, *op.cit.*, p.7.

¹¹²⁶ EDPB (2020) Guidelines 04/20, *op.cit.*, p.8.

¹¹²⁷ The EDPS, (2020) Tech Dispatch, Contact Tracing with Mobile Applications, Issue 1, p.3.

¹¹²⁸ EDPB (2020) Guidelines 04/20, *op.cit.*, p.8.

¹¹²⁹ See Article 6 of the GDPR, lawfulness of processing.

¹¹³⁰ See Article 6 of the ePrivacy Directive, traffic data.

useful in general, we are of the view that, from the controller's perspective, it seems to be bit vague and open to interpretation. It means that controller do know what they should do, but it seems bit high-level description, considering the significance of these points emphasized. Hence, it would be more plausible to indicate the potential boundaries, side effects of not providing elaborate purpose definition and legal basis of the applications. The lessons learned from this crisis are that EEA countries should review and adapt their laws, particularly with effective provisions such as those relating to the processing of health data for reasons of public health interest (Section Article 9(2)(i)).¹¹³¹ So far, few countries are using them for the benefit of research that contributes to public health, such as Belgium¹¹³², Slovenian¹¹³³ or Danish¹¹³⁴ application. This shows that many legislators and data protection authorities still do not fully understand the needs of health research and the reasons for the privileged status of scientific research under the GDPR.¹¹³⁵ Lessons learned from the COVID-19 crisis require the development of an operational framework that meets the needs of global research during the pandemic and provides legal certainty for researchers to act.

Moreover, with regards to the audits of the applications, the Guideline pointed out individuals who share information to do so with disclosure and consent around potential risks of private information that is subject to being shared. Automated decision-making driven contact tracing models could be hazardous for location data processing. Accordingly, the EDPB emphasizes that procedures and processes, including the algorithms used by contact tracking applications, should be overseen by trained and eligible persons to

¹¹³¹ Becker, Regina; Thorogood, Adrian; Ordish, Johan and Beauvais, Michael JS. (2020) "COVID-19 research: navigating the European general data protection regulation." *Journal of Medical Internet Research*, vol. 22, no. 8, e19799, pp.1-9, p.6.

¹¹³² See section 3 of the Corona Alert Privacy Statement, Limited processing for statistical purposes

¹¹³³ See Section 14 of the Privacy Policy of OstaniZdraw application, Statistics.

¹¹³⁴ See Section 3 of the Privacy Policy of Smittestop application, What is the purpose of our processing of personal data.

¹¹³⁵ Becker, Regina; Thorogood, Adrian; Ordish, Johan and Beauvais, Michael JS. (2020) "COVID-19 research....", op.cit., p.6.

avoid false positives and negatives.¹¹³⁶ Hence, the source code for the application should be made publicly available for scrutiny and review.¹¹³⁷ Algorithms should also be auditable and regularly evaluated by independent subject matter experts to guarantee their fairness, accountability, and, more generally, their conformity with the law as it now stands.¹¹³⁸ From our point of view, although data controller did not elaborate any audit mechanism, probably because they were not able to oversee the duration of the processing activities, it should be evaluated with DPIA requirement as a two-fold approach. For DPIA requirement, the guideline pointed out the fact that DPIAs should be published as much as possible. This is what we discussed in the relevant section of Chapter 4, as we thought that it is an important tool to solidify user trust. Nevertheless, we must reiterate that there is a still room for improvement for data controllers for this task. The fundamental reason is, first of all, not all of them published their DPIAs, except Poland, Germany, Belgium, Austria, Portugal, Denmark, Finland, Norway, France, Ireland, applications, as detailed in Chapter 4. Yet, above all, not all of the controllers review their DPIAs, in light of the evolving nature of the pandemic and technical vulnerabilities, given that pandemic did last for more than two years.

From the legal perspective, we are of the view that, as elaborated in Chapter 2, re-identification and location tracking are the major data protection concerns associated with the use of the applications. Hence, it is plausible to emphasize the importance of strict data protection requirements resulting from the legislation. On the top of that, setting out ground rules, and defining the limit of data processing activities from purpose perspective as advised by the ICO, is an important action to avoid any sort of feared events,¹¹³⁹ which we find quite positive from the regulatory perspective. Additionally, with

¹¹³⁶ EDPB (2020) Guidelines 04/20, *op.cit.*, p.9.

¹¹³⁷ ICO guidance COVID-19 Contact tracing: data protection expectations on app development *op.cit.* p.7.

¹¹³⁸ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

¹¹³⁹ ICO, Purpose limitation, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/> (accessed on 23 June 2024).

regards to the implementation of this necessity by the controllers, based on the technical specifications of their applications, as well as their privacy policies, they refrained from processing identifiers, thereby they implemented unique and pseudonymous identifiers in line with the guideline. In line with this perspective, The EDPS emphasized that effectively anonymized data do not fall under the purview of data protection laws with regard to the use of location data for mapping the pandemic's spread and emphasized the significance of putting in place the necessary safeguards to ensure the safe transmission of data from telecom providers, by specifying that these special services were only being used temporarily and had only been brought in due to the current crisis¹¹⁴⁰. Or else, even better for the full guarantee of feared events detailed, the Guideline praised the plan to erase the information collected from cell operators as soon as the immediate situation was resolved.¹¹⁴¹ According to the EDPS, such advances typically do not provide people the option of backing out when an emergency arises.¹¹⁴²

Subsequently, regarding one of the hottest debates on the technical aspect, namely architectures of the applications, the EDPB recommended the adoption of both centralized and decentralized systems, provided that adequate security measures are implemented.¹¹⁴³ Proceeding with the same logic, for instance, it also mentioned the importance of certain limitations regarding the type of data broadcasted by applications. That is to say, as long as it merely contains certain unique and pseudonymous identifiers, created by and particular to contact tracing applications, and those identifiers should be refreshed on a regular basis, and enough to restrain identification and of physical tracking of data subjects related risks.¹¹⁴⁴ This perspective brought by the Guideline has opened a door for efficient implementation of the

¹¹⁴⁰ Kędzior, Magdalena (2021) "The right to data protection and the COVID-19 pandemic: the European approach." *ERA forum*, vol. 21, no. 4, Springer, pp. 533-543, p.535.

¹¹⁴¹ *Ibid.*, p.536.

¹¹⁴² *Ibid.*, p.537.

¹¹⁴³ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

¹¹⁴⁴ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

technical and organisational measures set out in the GDPR¹¹⁴⁵ by prioritizing the measures over the one-sided applications. This perspective has been used for data transfer agreements, in particular standard contractual clauses of the Commission is a good sample, which prioritizes the essence of technical and organisational safeguards¹¹⁴⁶ without limiting the transfer by other technical and organisational measures. It, therefore, could pave the way for the use of centralized apps such as France, Hungary, and Norway apps, as long as they adhered to the requirements set out in the Guideline and the GDPR.

Furthermore, establishing a comprehensive global contact tracing method, involving both applications and manual tracing, might necessitate processing additional information in certain scenarios. In such cases, this extra information should stay on the user's device and only be processed when absolutely essential and with their explicit and prior consent. While many are reluctant to allow the health system to use their data for exposure tracking purposes, the EDPB stresses that consent is not the best basis for authorities.¹¹⁴⁷ Consent given to public authorities is generally not considered freely given, because public authorities have the power or potential power to enforce compliance.¹¹⁴⁸ Users can withdraw their consent at any time, but withdrawing consent after notification of a positive diagnosis could jeopardize the mission of public health agencies. Instead, the EDPB clarified that the authorities would most likely rely on Article 6(1)(e). Furthermore, on the top of these challenges, it is quite difficult to manage and track the consent of the users, as detailed in the next section, and in Chapter 3, due to time-consuming

¹¹⁴⁵ See Article 32 of the GDPR, security of processing.

¹¹⁴⁶ See EU Commission, Standard Contractual Clauses for Data transfer between EU and Non-EU Countries, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on 8 July 2023).

¹¹⁴⁷ Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps...", op.cit., p.13.

¹¹⁴⁸ Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps...", op.cit., p.13.

nature, which hampers the efficiency of the processing activities to some extent.

Nevertheless, as a good sign of compliance from the data controllers side, controllers implemented data protection requirements to obtain informed consent from individuals before collecting their location data or engaging them in contact tracing, as their website notices, terms and conditions documentation, and technical specifications are detailed, and supported by the elaborate Q&A, which is perfectly indicating the requirements of consent guideline of the EDPB, as user control is rendered meaningless and consent is rendered ineffective if the controller does not make information accessible.¹¹⁴⁹ Furthermore, from the voluntariness- #consent relationship perspective highlighted by the Guidelines, controllers also reiterated that individuals should have the right to withdraw their consent at any time without facing consequences.

Similarly, consent discussions would lead us to on the lawful basis discussions. As a potential alternative to stretching the legal boundaries of the applications by the controllers, governmental agencies have developed guidelines to address data analysis procedures during the Covid-19 outbreak, contending that privacy and health protection may coexist. In order to combat the spread of the virus, the Committee of the Global Privacy Assembly (GPA) supported governments and organizations by issuing a directive in March 2020.¹¹⁵⁰ The approach used by national data protection agencies, including the EDPB, the CNIL in France, the ICO in the UK, and the FDPIC in Switzerland, is consistent with this GPA instruction.¹¹⁵¹ To be more specific, as long as the GDPR principles outlined above are followed to the greatest extent possible, the actions necessary to contain and fight the spread of such

¹¹⁴⁹ EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679, p.15.

¹¹⁵⁰ Newlands, Gemma; Lutz, Christoph; Tamò-Larrieux, Aurelia; Fosch Villaronga, Eduard; Harasgama, Rehana and Scheitlin, Gil (2020) "Innovation under pressure: Implications for data privacy during the Covid-19 pandemic", *Big Data & Society*, vol. 7, no. 2, 2053951720976680, pp.1-14.

¹¹⁵¹ *Ibid.*

a pandemic must be implemented in Europe. This is the case even if there is no overriding public or private interest.

Therefore, we are of the view that data controllers did act in with a good manner, not to take advantage of this situation based on their detailed privacy-by-design approach documented on their policies and technical specifications. The fundamental reason is, considering that data controllers were public institutions as well, they could exert their power on data supervisory authorities to issue a directive on the direction, which is more application friendly, rather than privacy friendly perspective. Particularly, the Constitution and human rights were established with such a crisis in mind.¹¹⁵² Moreover, the International Covenant on Civil and Political Rights (ICCPR)¹¹⁵³ and at the European level the European Convention on Human Rights (ECHR) are also actively dealing with such complicated situations. When looking at these developments from a formal perspective, it makes sense to consider the legal and institutional framework of the Council of Europe (CoE). Accordingly, the Council of Europe has established procedures and jurisprudence in times of crisis. The Guide to Article 15 ECHR on Emergency Exceptions was recently updated on 31 December 2019 (Council of Europe/European Court of Human Rights 2019)¹¹⁵⁴. As per the document, states may make exceptions in the following circumstances:

- wars and other public emergencies threatening the lives of citizens.
- to take action that is absolutely necessary due to the urgency of the situation.

¹¹⁵² Zwitter, Andrej and Gstrein, Oskar Josef (2020) "Big data, privacy and COVID-19—learning from humanitarian expertise in data protection", *Journal of International Humanitarian Action*, vol. 5, no. 1, pp. 1-7, p.2.

¹¹⁵³ See the International Covenant on Civil and Political Rights (ICCPR), entry into force: 23 March 1976, in accordance with Article 49 available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

¹¹⁵⁴ See the Guide to Article 15 ECHR on Emergency Exceptions, Derogation in time of emergency, December 2019 available at: https://www.echr.coe.int/documents/guide_art_15_eng.pdf.

- provided that such measures are consistent with other obligations under international law.

However, from our angle, as a positive outlook, neither data supervisory authorities nor data controllers tried to stretch the boundaries of the general processing principles of the GDPR¹¹⁵⁵ and ePrivacy Directive¹¹⁵⁶, which we believe that it was in the spirit of the European approach for protection of human rights of privacy. Their privacy-by-design endeavours, as per their privacy policies, and terms and conditions documentation, seemed to incentive controllers from the beginning not to ramble from privacy-friendly approach, which is in line with the European data protection law perspective, as detailed in Chapter 4, and with the Guidelines as well.

Mentioning of privacy-by-design approach of the controllers, with regards to the retention periods of the personal data at stake, the Guideline pointed out cutting-edge cryptographic methods should be performed to safeguard the stored data in applications and servers, which is being exchanged across the applications and the remote server.¹¹⁵⁷ To this end, we believe that the approach of controllers are also positive in this regard, as robust cryptographic measures were implemented to protect the collected data from unauthorized access or breaches based on their privacy policies. Also, almost each controller emphasized the importance of strong encryption protocols, secure data storage practices employed to minimize the risks associated with data handling and storage, as detailed in previous chapters, in line with the Guideline. More on the matter, as stated above, being cutting-edge for the implementation of required security and legal measures is incentivized for almost each part of the processing activities, including but not limited to storage of personal data.

¹¹⁵⁵ See Article 5 to 11 of the GDPR, principles.

¹¹⁵⁶ See Article 4 and 5 of the ePrivacy Directive, security and confidentiality.

¹¹⁵⁷ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.9.

Having said that, this approach, i.e., being cutting-edge, also seems to be bit limited and open ended, as the term of state-of-the art¹¹⁵⁸ is evolving, and since it is a subject specific guideline, it must evaluate the type of these state of the art cryptographic methods. In other words, for the regulatory part, we can assume that it is not a straightforward task to do it in one single document to list any potential cryptography technology. Nevertheless, from our perspective, to make it more digestible to the data controllers, it is always good to publish series of documents under this umbrella guideline, to deep dive on each aspect on quarterly basis. This, we believe, would be in line with the evolving nature of the technological developments, whereas at the same time keeps serving to the utmost data protection activities on the legal side. However, this determination is not specific to retention of personal data in servers, but rather as a holistic view of the situation which guideline aims to reach. In other words, we believe that regular security audits should be implemented from both legal and technical side of data protection, if such dynamic approach is aimed by the EDPB and the Commission.

Therefore, we are of the view that the guideline would be more interesting and pioneer, if there were further deep dive on the each legal breakdown of the each requirement and potential intrusiveness thereof, as per the main points relating to the applications set out in the GDPR¹¹⁵⁹ and ePrivacy Directive, it would be more robust baseline for the controllers to build thereupon. Having said that, as it is already overarching enough to cover various aspects of the data protection regime to which data controllers must adhere, it is on the other hand provides with certain “not-to-dos”, rather than “to-dos”. This prohibitive approach, we believe, is in line with the imperative nature of the data protection laws and regulations in Europe, given that the European legislation is maintaining the most meticulous and mindful approach against any sort of privacy intrusive acts of the controllers. Furthermore, it might be creating

¹¹⁵⁸ This term “state-of-the-art” is used in article 32 of the GDPR, while describing the nature of the sufficient technical and organizational measures to provide a level of security.

¹¹⁵⁹ See Article 32 of the GDPR, security of processing.

another discussion around term of “legal psychology”.¹¹⁶⁰, considering that law also imposes practical requirements (e.g., providing informed consent, record keeping, confidentiality, patient rights to refuse service, etc.).¹¹⁶¹ Particularly, when we consider these days, psychologists are now studying law in an effort to enhance the legal system by applying their knowledge there.¹¹⁶² The goals of both disciplines could be accomplished if legal and psychological research acknowledges the special challenges that the psychological study of law presents.¹¹⁶³ Although it does not fall within the scope of this research, we believe it is still worth touching the interplay between both fields briefly, to indicate the outcome of the perspective brought by the EU institutions from data controllers’ perspective as targeted by this thesis.

On the other hand, data controllers might feel the lack of elaborate approach provided on advisory role of the Guideline, as it is rather succinct and high-level for some points delineated. Hence, from our perspective, to strike the balance between both approaches, the EDPB took a mixed stance on this matter. To be more concrete, on the contrary of the legal analysis and technical requirements parts, it provided more overarching appendix comprising detailed steps that must be taken and things that must be refrained by data controllers of the applications. To this end, it specified the many steps, including but not limited to data protection necessities, technical and functional necessities, purpose limitation and so forth¹¹⁶⁴. Even more notably,

¹¹⁶⁰ Regarding the terminology of Legal Psychology, as per the definition used by Konečni, Vladimir J., and Ebbesen, Ebbe B. the primary aim of this discipline is to investigate various aspects of the "interface" between psychology and law. Specifically, it seeks to improve the understanding of how the legal system functions by employing psychological research methods and testing the validity of psychological assumptions embedded in legal statutes or used by legal practitioners on an ad hoc basis. For the full study see Konečni, Vladimir J., and Ebbesen, Ebbe B. (1979) "External validity of research in legal psychology." *Law and Human Behavior* 3, no. 1-2, pp.39-70, p.39.

¹¹⁶¹ Sales, Bruce D., and Daniel A. Krauss. (2015) “*The psychology of law: Human behavior, legal institutions, and law*”, American Psychological Association, p.20.

¹¹⁶² Dash, Sidhartha Sekhar and Modi, Ronak, (2019) “Role of Psychology in Legal Studies”, *JETIR*, Vol. 6, Issue 5, pp.2557-2562, p.2562.

¹¹⁶³ *Ibid.*

¹¹⁶⁴ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.12 to 17.

it made a distinction between the principles that solely apply when the application transmits a roster of contacts to the server and those that are relevant only when the application sends its own identifiers to a server, which we find quite enlightening and meticulous, and it is truly what is expected by means of guideline for the controllers¹¹⁶⁵. By such a detailed approach, data controllers would be able to better position themselves against any sort of ambiguous part of the implementation of data protection necessities.

As mentioned, some of these more elaborated explanations are in the form of not-to-dos”, whereas the other part thereof is “to-dos”, which we find quite positive to strike the aforementioned balance between the spirit of the regulations and being the best practice of each data controller in Europe. As much as controllers seem to fulfil their many of duties resulted from the GDPR as detailed in the previous two chapters, some of the applications such as Estonian¹¹⁶⁶ or Norwegian¹¹⁶⁷ applications seem to have fallen short of indicating their success on some of the steps they implemented, although they were successful. To be completely fair, in privacy practice, it would also be unrealistic assume that each controller act in a cadence and impeccability against the one of its kind sort of pandemic with the amount of massive uncertainty, still some of the applications at least raised the bar for the others too such as Italian¹¹⁶⁸, Croatian¹¹⁶⁹, German¹¹⁷⁰, Slovenian¹¹⁷¹ applications,

¹¹⁶⁵ EDPB (2020) Guidelines 04/2020, *op.cit.*, p.18.

¹¹⁶⁶ HOIA Phone Application Privacy Policy, <https://koodivaramu.eesti.ee/tehhik/hoia/app-web/-/blob/master/content/privacy.en.md> (accessed on 23 June 2024).

¹¹⁶⁷ Smittestopp Privacy Policy, available at <https://www.fhi.no/en/about/smittestopp/use-of-smittestopp-privacy-policy> (accessed on 11 January 2024).

¹¹⁶⁸ Immuni Application Documentation <https://github.com/immuni-app/immuni-documentation#privacy> (accessed on 23 June 2024).

¹¹⁶⁹ Stop Covid Privacy Notice <https://stopcovid19.zdravlje.hr/html/privacy-policy.html> (accessed on 10 August 2022).

¹¹⁷⁰ Corona Warn, Privacy <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).

¹¹⁷¹ Ostani Zdrav, Functioning of the application <https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanzdrav-mobile-application/functioning-of-the-application/>. (accessed on 23 June 2024).

among others, which automatically changed the assessment of the other scholars and data subjects against these apps too. Still, overall, our assessment on the data controller side is positive for the implementation of the guidelines, particularly regarding the aspects delineated. That being said, for the regulators/authorities, we must reiterate that this Guidance could be more elaborate and published as part of ongoing series, so that we could have a better chance to examine controllers' ongoing compliance with the each data protection requirements within the scope of pandemics.

2. EU Toolbox for Contact Tracing Applications (eHealth Network)

With regards to the guidance eHealth Network, mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States¹¹⁷², eHealth Network¹¹⁷³ provided an overview on common approach, and certain recommendations on technical feasibility, cybersecurity, privacy-preserving approach and interoperability of the applications. Overall, the document is extensive and elaborated the each aspect of the contact tracing data protection requirements in Europe, and starting from the backwards of our assessment of the guidance, it is possible to mention that the toolbox focuses on a variety of themes and concerns, from privacy, which is covered in more detail in a second document, to the cybersecurity aspect, as it addresses the development of contact tracing applications.¹¹⁷⁴

¹¹⁷² eHealth Network (2020) "Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States" (hereinafter will be referred to as the "Guidance" through this section).

¹¹⁷³ As Per the Guidance definition "The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with digital health. The Joint Action supporting the eHealth Network (eHAction) provides scientific and technical support to the Network".

¹¹⁷⁴ Ravizza, Alice; Sternini, Federico; Molinari, Filippo; Santoro, Eugenio and Cabitza, Federico (2021) "A proposal for COVID-19 applications enabling extensive epidemiological studies", *Procedia computer science*, vol.181, pp 589-596, p.592.

Particularly, with regards to the cyber security aspect of the apps, the eHealth Network took the similar stance what we discussed earlier in Chapter 2 and 4, regarding the relation of both fields. Accordingly, given that cybersecurity of these mobile applications, backends and all related services is extremely important, Member State authorities and developers of these applications should therefore take a range of measures to ensure adequate cybersecurity throughout the application lifecycle. To this end, the cybersecurity requirements detailed in Annex 1 of the document, which was provided by ENISA, the EU Agency for Cybersecurity¹¹⁷⁵, and based on current best practices as regards the secure design, development, and deployment of mobile applications, in line with our stance for inclusion of cyber security experts into the design and implementation process of the application for national authorities, as previously discussed.

From data protection law perspective, we believe that it is the right direction of the travel to act in line with the evolving nature of the technology and pandemic, by setting up a detailed analysis. Also, to go one step further, as discussed in Chapter 4, we presented a solution for controllers to track these novelties and implementing the due care against new cyber, thereby data protection related threats by establishing taskforce, and complement these acts with advisory activities from private/public institutions. Accordingly, regulators' approach seems to be in line with the reality of the pandemic and technology, and therefore we positive evaluate such elaborated perspective. On the other hand, apart from few data controllers, as per the EU data, such as Estonia, Denmark, Portugal, German, French, the Dutch, Finland and Irish,

¹¹⁷⁵ The European Union Agency for Cybersecurity (ENISA) collaborates with Member States and EU bodies, contributes to EU cyber policy, improves the trustworthiness of ICT products, services, and processes through cybersecurity certification schemes, and aids Europe in preparing for future cyber challenges. For further details on the activities of ENISA, see <https://www.enisa.europa.eu/> (accessed on 15 July 2023).

based on the EU Commission data, we could not simply conclude that such cyber security related approach was reflected on controllers.¹¹⁷⁶

Subsequently, the common toolbox emphasized the use of two predominant privacy preserving solutions, which we find quite efficient for the purpose of solidifying privacy-preserving approach to be taken by the controllers.¹¹⁷⁷ These are namely, decentralized solution and backend server solution, with nuance differences.¹¹⁷⁸ In other words, the Toolbox tends to propose a decentralized approach, in line with previous committee letters.¹¹⁷⁹ However, this document also includes a discussion of an alternative centralized model where arbitrary identifiers are uploaded to the health authority's backend his server.¹¹⁸⁰ Furthermore, on the top of both solutions emphasized, i.e., decentralized solution and backend server solution, the toolbox indicated that the option of centrally storing directly identifiable data about each individual who downloads an app by health authorities includes the EDPB in its response to consultations on draft European Commission guidelines on privacy and app tracking. As such, it has been pointed out that there are

¹¹⁷⁶ For the inclusion of cybersecurity committees, national authorities, private cyber security companies see European Commission (2022) "Digital Contact Tracing Study on lessons learned, best practices...", op.cit., p.123 to p.190.

¹¹⁷⁷ Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps...", op.cit, p.27.

¹¹⁷⁸ Bradford, Laura; Aboy, Mateo and Liddell, Kathleen Liddell (2020) "COVID-19 contact tracing apps...", op.cit., p.27.

¹¹⁷⁹ Lomas, Natasha (2020), "EU lawmakers set out guidance for coronavirus contacts tracing apps" Tech Crunch available at: <https://techcrunch.com/2020/04/16/eu-lawmakers-set-out-guidance-for-coronavirus-contacts-tracing-apps/> (accessed on 15 June 2024).

¹¹⁸⁰ *Ibid.*

serious shortcomings.¹¹⁸¹ These options do not limit the processing of personal data to an absolute minimum and may discourage users from installing and using our apps.¹¹⁸²

Interestingly, the views presented by the EDPB Guideline, and the Toolbox are conflicting with each other in terms of the use of architectural design of the applications from data protection perspective. The reason is Toolbox seems to be more focus on technical data protection necessities for the architectural design of the applications, rather than legal safeguards. Particularly, regarding the cyber security necessities, although it is quite a high-level, it is still creating a standpoint for the personal data breaches and cyber-attacks resulting from the storage of excessive personal information related to data subject users. Cross referencing to the Commissions' draft guidance, which will be later reviewed in this chapter, is a successful indication of acting in harmony with the consolidated approach of the EU institutions dealing with data protection law. However, regardless, our approach is in line with what data controllers provided on this issue, namely if controllers are providing the most efficient legal and technical safeguards, they should be indifferent between the architectural choice of the applications. With regards to the further data processing activities, which remain bit ambiguous from our perspective throughout the use of the apps, the toolbox pointed the direction of opt-in requirement, which some of the data controllers

¹¹⁸¹ For the full decision see EDPS comments on the Commission draft implementing decision amending Implementing Decision 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. https://www.edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-cross-border-exchange-data-between_en (accessed on 5 June 2024).

¹¹⁸² EDPS comments on the Commission draft implementing decision amending Implementing Decision 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. https://www.edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-cross-border-exchange-data-between_en (accessed on 5 June 2024).

such as the Dutch¹¹⁸³, Spanish¹¹⁸⁴, Danish¹¹⁸⁵ and Belgium¹¹⁸⁶ applications, followed too. However, again, not all the controllers relied on detailed opt-in mechanism. We, thus, believe that this created a balanced perspective, with regards to the implementation of both logics, i.e. strict application of not processing of identifiable data, and freedom of providing further data on “voluntary” basis by implementing opt-in mechanism. In more detail, they proposed that while not essential for the app's operation, an individual alerted of contact with a positively tested person might desire to share personal information with public health authorities for additional assistance and guidance. The app could include an option to facilitate this process. This should be an “opt in” option and clearly indicated as “opt in”. The authority can then contact the individual and advise him or her accordingly. This is certainly compatible with the study of Fox and colleagues, which mentions in case individuals believe their loved ones, such as colleagues, friends and family, will appreciate their decision to download a contact tracing app, they are more likely to download the app.¹¹⁸⁷ A form of social influence, the role of reciprocity is closely related to the issue of social influence.¹¹⁸⁸ Reciprocal awareness, by accepting applications and disclosing information, signals to an individual that others also accept some vulnerability, positively influencing the evaluation of that person's behaviour, Increases willingness to participate in problem behaviour.

Correspondingly, we also believe that, based on the applications' privacy policies, emphasize on consent by the eHealth guidance is of importance for

¹¹⁸³ See Corona Melder Privacy Policy, *op.cit.*, Section 3.

¹¹⁸⁴ See Radar Covid Privacy Policy, *op.cit.*, Section 4.

¹¹⁸⁵ See Smittestopp Processing of Personal Data, *op.cit.*, Section 4.

¹¹⁸⁶ See Corona Alert, Privacy Statement, *op.cit.*, Section 3, para 1,

¹¹⁸⁷ Fox, Grace; Clohessy, Trevor; van der Werff, Lis; Rosati, Pierangelo and Lynn, Theo (2021) "Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications" *Computers in Human Behavior*, vol.121, 106806, pp.1-15, p.10.

¹¹⁸⁸ Fox, Grace; Clohessy, Trevor; van der Werff, Lis; Rosati, Pierangelo and Lynn, Theo (2021) "Exploring the competing influences ...", *op.cit.*, p.10.

the indication to the consensual application of the apps from the data protection and surveillance point of view, considering A maximum of citizens must be persuaded to be interested in using such an app, and any obstacles to app use must be eliminated.¹¹⁸⁹ This is certainly important signal for the any data subject planning to use the applications, and additionally it creates a positive attitude among users for affirming the use of the apps. Particularly, this is becoming more valid, considering that a centralized database is not a privacy-preserving tool for contact tracking, because giving the government access to the central server would effectively turn it into a surveillance tool.¹¹⁹⁰ The similar is also raised in Tech Dispatch publication of the EU¹¹⁹¹, which, from our perspective, is the most valid and fundamental concern among the risks, therefore, upon which a lot of discussion should be made by the authorities.

On the top of that, as a positive side for the toolbox of this approach, it did not recommend a one-valid-for all approach, but rather leave the freedom for both controllers and data subjects if they stay within the boundaries of the fundamental data protection law principles. On the other hand, it would raise a scepticism whether it was to be interpreted as potential way to identify and store personal data as detailed in Chapter 2 but considering that the toolbox lay down the ground rules, it does seem realistically possible for controllers to act in such an abusive way. Therefore, in short, we really appreciate the emphasize on opt-in mechanism, which we highlighted the importance thereof in previous chapters as well.

From our perspective, as a general overview of the toolbox, all these high-level approaches are supported with more detailed solutions and information in the end of the document, as an annex. This is certainly very much important

¹¹⁸⁹ Touzani, Rajae; Schultz, Emilien; Holmes, Seth M.; Vandentorren, Stéphanie; Arwidson, Pierre; Guillemain, Francis; Rey, Dominique; Rouquette, Alexandra; Bouhnik, Anne-Déborah and Mancini, Julien (2021) "Early acceptability of a mobile app for contact tracing during the COVID-19 pandemic in France: National web-based survey", *JMIR mHealth and uHealth*, vol. 9, no. 7, e27768, pp.1-13, p.2.

¹¹⁹⁰ Ogbuefi, Nnubia. (2021), "Contact Tracing and Its Approach to Privacy....." op.cit., p.21.

¹¹⁹¹ The EDPS, (2020) Tech Dispatch, Contact Tracing with Mobile Applications, Issue 1, p.3.

step against the creation of credible and reasonable solutions. Particularly, it is also important to indicate the controllers that they are not left alone to navigate their route as per the overarching principles of the GDPR¹¹⁹² and ePrivacy directive¹¹⁹³ for the security matters¹¹⁹⁴, but rather creating bespoke and detailed solution for everyone involved in the processing activities by delineating the technical and legal implementation of each plausible scenarios and requirements. We need to mention the fact that our examination of the toolbox is merely limited to the data protection, cyber security and legal aspects set out in the document in line with the research topic of our thesis, rather than each technical and administrative merits provided. Therefore, what we are providing as an assessment of these matters does not necessarily need to reflect the technical and administrative success of the toolbox, although most of the data controllers, such as Italian¹¹⁹⁵, Irish¹¹⁹⁶, French¹¹⁹⁷, Slovenian¹¹⁹⁸, German¹¹⁹⁹ applications, provided extensive information about the technicalities relied during the use of the applications, which is certainly privacy-friendly actions from our point of view.

As a criticism, which could have been remediated via specification of relevant actors of supporting actions dealing with the safeguards of the application, there is a bit of ambiguity around target audience, namely the ones who is

¹¹⁹² See article 32 of the GDPR, security of the processing.

¹¹⁹³ See recital 83 of the GDPR. General conditions for imposing administrative fines.

¹¹⁹⁴ See article 4 of the ePrivacy Directive, security.

¹¹⁹⁵ See Immuni App, Technical Documentation, op.cit., section “how it works”.

¹¹⁹⁶ For the full document and detailed data protection specifications, HSE data protection policy, <https://www.hse.ie/eng/gdpr/hse-data-protection-policy/> (accessed on 23 June 2024).

¹¹⁹⁷ For the full document and detailed technical specifications see Tous Anti-Covid, Technical Specifications, pp. 3-10.

¹¹⁹⁸ For the full document and detailed technical specifications see Ostani Zdrav, Functioning of the application, <https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanizdrav-mobile-application/functioning-of-the-application/> (accessed on 23 June 2024).

¹¹⁹⁹ For the full document and detailed data protection architect, see Corona Warn, Solution Architect https://github.com/corona-warn-app/cwa-documentation/blob/main/solution_architecture.md#mobile-applications (accessed on 23 June 2024).

going to perceive and implement as necessary. It is devoted to data controllers, but still it would be better indicated by specifically targeting the ones who need to implement it by providing even breakdowns for each specific type of data controller, i.e., health authorities, central governments, etc. Nonetheless, in general, the approach and amount of detail provided for each step is quite positive.

As an efficient approach, as briefly touted in the introduction of this section, the eHealth network specified certain cyber security requirements for national health authorities and data protection requirements for the controllers as well. Regarding cyber aspect, the guideline stated the importance of the national authorities undertaking a holistic risk assessment focused on the potential cybersecurity risks of COVID-19 applications, considering known security issues in underlying platforms and communication protocols, current incidents and threats. should be implemented.¹²⁰⁰ Relevant portions of this national risk assessment should be shared with the project team developing application.¹²⁰¹ The reasoning of this perspective is ensuring data integrity, confidentiality, and secure storage minimizes the risk of unauthorized access or breaches. To this end, the Toolbox emphasized data minimization and minimum permissions, secure software development, built-in security for apps, protocols, and backend. communication security, encryption, cryptography, secure-by-default, and user friendly, user authentication.¹²⁰² Hence, it is plausible to state that the Toolbox underscores the need for robust security measures, including strong encryption protocols, to protect the data transmitted and stored by contact tracing applications.

Regarding the response of data controllers such requirements, as these parts are already detailed in previous Chapters, as a pleasing indicator of the compliance therewith, data controllers' policies and website documents are indicating the controllers' positive attitude in line with the many aspects of this

¹²⁰⁰ Toolbox, *op.cit.*, p.33.

¹²⁰¹ Toolbox. *op.cit.*, p.34.

¹²⁰² Toolbox, *op.cit.*, p.35.

guidance as well. To be more specific, we believe that aforementioned data protection related technical necessities were elaborated in their privacy policies, which solidifies the legal implementation of such measures as well. From the legal perspective, this detailed approach brought by eHealth Network, has also triggered the approach discovered by the EU Commission's progress report¹²⁰³, explore cutting-edge and privacy enhancing technical solutions In April 2020, the European Commission launched a collaborative environment to support the technical evaluation of proposed technologies to combat COVID-19 in terms of effectiveness, security, privacy, accessibility, and interoperability. Call for tenders for establishment, maintenance and operation has been opened by EU toolbox compliance.¹²⁰⁴

Lastly, from the legal perspective, considering the GDPR and ePrivacy Directives, eHealth Network also followed their fundamental principles of security of processing articles¹²⁰⁵ with nuance differences by setting out the importance of encryption, pseudonymization, data deletion, etc., as elaborated in privacy by design and default sections, data controllers' outlook were positive against legal and data protection related parts set out in the guidance in general as they provided these high level requirements. However, more to this requirement, the Toolbox highlights the importance of transparency in the use of contact tracing applications. Governments and app developers should provide clear information about data collection, storage, retention, and deletion practices, which was also raised a fundamental concern in Tech Dispatch publication of the EU.¹²⁰⁶

Additionally, as we already supported from the beginning of this research that certain mechanisms for accountability, such as independent audits or oversight bodies, should be established to ensure compliance with privacy

¹²⁰³ Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, op.cit., p.1.

¹²⁰⁴ Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020, op.cit., p.15.

¹²⁰⁵ See article 32 of the GDPR, security of processing.

¹²⁰⁶ The EDPS, (2020) Tech Dispatch, Contact Tracing with Mobile Applications, op.cit., p.3.

regulations. This approach articulated explicitly by the Toolbox, about which, hence, our assessment is completely positive. The underlying reasoning thereof is that the Toolbox acknowledges the importance of user empowerment, granting individuals control over their personal data.¹²⁰⁷ Contact tracing applications should allow users to access, review, correct, and delete their data, ensuring they can manage their privacy. This is certainly in line with our perspective delineated in Chapter 3, with regards to the implementation of data subject rights set out in the GDPR¹²⁰⁸, by prioritizing the sense of legal accountability over the technical efficiency of the application, which we think is quite plausible and in line with the general European approach as well. Hence, an independent oversight mechanism would radically enhance the capabilities of the data controllers. Further input with regards to the significance of the transparency requirements set out in the GDPR, which we deem cutting-edge solution to the acceptance of the applications, the study of Kolasa and colleagues' indicated that a prima facie study implies that the data's value to public health increases with how much the government intrudes on people's privacy.¹²⁰⁹ Furthermore, it appears that using data for public health purposes is hampered by a high level of privacy protection. However, we contend that it is possible to view the two interests as complementary. Adoption of transparency rules that boost confidence between public and private stakeholders should be advocated to accomplish this goal.¹²¹⁰ In fact, strong public trust in digital solutions created by governments that emphasize defending citizens' rights might encourage further data sharing for public health purposes, among other things. Such

¹²⁰⁷ Toolbox, *op.cit.*, p.35.

¹²⁰⁸ See GDPR, Articles 12 to 23.

¹²⁰⁹ Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review." *JMIR mHealth and uHealth* 9, no. 6, e23250, p.7.

¹²¹⁰ Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the art ...", *op.cit.*, p.7.

approach could have been advertised by the guidance as well, in addition to what is provided by the guidance on a high-level.

Overall, the general attitude of the eHealth Network regarding the technical and data protection law related aspects as well as cyber security related measures are elaborated, and unique, in comparison with the other guidance/guidelines analysed in this Chapter, which creates less room for mistake from the controllers. Having said that, there are still some parts from the regulatory perspective, which could be subject to further improvement such as the absence of more detailed legal framework or the necessities, which was detailed above. Similarly, controllers' act was also not entirely in line with the Toolbox Nevertheless, due to the aforementioned missing parts. Thus, in general, it is fair to conclude that data controllers seemed to implement their duties precisely other than few aspects, from implementation perspective of the data protection law requirements of the Guidance.

3. Communication From The Commission - Guidance On Apps Supporting The Fight Against COVID 19 Pandemic In Relation To Data Protection (2020/C 124 I/01)

Similar to the guidelines examined in section 1 and 2 of this Chapter, the Guidance of EU Commission also sets out its direction by stating the GDPR and the ePrivacy Directive are two pieces of personal data protection legislation that must be complied with by apps in order to be compliant with EU privacy and personal data protection laws.¹²¹¹ Therefore, the guidance stated that this guidance therefore outlines the features and requirements that apps must meet to do so. It also offers guidance to Member States and app developers.

With regards to the legal foundation on which the guidance built, the guidance indicated that a variety of rights enshrined in the EU Charter of Fundamental Rights, including, respect for private and family life, human dignity, protection of personal data, non-discrimination, freedom to operate a business, freedom of movement, and freedom of assembly and association, may be affected in

¹²¹¹ Coronavirus: Guidance to ensure full data protection standards of apps fighting the pandemic, p.2.

different ways by the functionalities included in the apps.¹²¹² We are of the view that, such approach brought by the recommendations is of importance to the long-lasting efficiency versus privacy discussion. As also supported by the Osman and colleagues that privacy issues include both behavioural and technical issues.¹²¹³ However, policymakers need to balance the effectiveness of contact tracing apps with public privacy, raising certain deceit issues.¹²¹⁴ Therefore, the fact that some of the features are based on a data-intensive model raises the possibility that the invasion of privacy and the right to the protection of personal data will be especially relevant.¹²¹⁵ To this end, the Commission indicated that the elements listed below are intended to serve as guidelines for how to ensure compliance with EU personal data protection and privacy legislation by limiting how intrusive the app's functionality can be.¹²¹⁶

To being with, the recommendation also set out with regards to the legal basis that, a particular functionality may be implemented on the user's device, potentially requiring the infected or likely infected user to upload proximity data.¹²¹⁷ However, such an upload is not essential for the proper functioning of the application itself, thereby failing to meet the requirements of option (ii) mentioned earlier. Consequently, as per the Guidance, consent (option (i)) becomes the most appropriate legal basis for the pertinent activities. This consent must be freely given, specific, explicit, and informed in accordance

¹²¹² Guidance to ensure full data protection *op.cit.*, p.3.

¹²¹³ Osman, Magda; Fenton, Norman Elliot; McLachlan, Scott; Lucas, Peter; Dube, Kudakwashe; Hitman, Graham; Kyrimi, Evangelia; and Neil, Martin (2020) "The thorny problems of Covid-19 Contact Tracing Apps: The need for a holistic approach", *Journal of Behavioral Economics for Policy*, vol.4, no. S, pp. 57-61, p. 58.

¹²¹⁴ Osman, Magda; Fenton, Norman Elliot; McLachlan, Scott; Lucas, Peter; Dube, Kudakwashe; Hitman, Graham; Kyrimi, Evangelia; and Neil, Martin (2020) "The thorny problems of Covid-19", *op.cit.*, p. 58.

¹²¹⁵ Guidance to ensure full data protection, *op.cit.*, p.3.

¹²¹⁶ Guidance to ensure full data protection, *op.cit.*, p.4.

¹²¹⁷ Guidance to ensure full data protection, *op.cit.*, p.5.

with the GDPR requirements.¹²¹⁸ It should be expressed through a clear affirmative action by the individual, excluding tacit forms of consent like silence or inactivity, as recommended by the EDPB consent guideline.¹²¹⁹ Therefore, from the regulator perspective, the applicability of the consent options has been prioritized and not drastically changed from the general implementation of the consent, which is in contradiction with the general implementation of the lawful basis by data controllers, as elaborated in Chapter 3.

In the same respect, it is also elaborately indicated in Chapter 3 that the legal basis for processing personal data by national health authorities is typically determined by EU or Member State law, and these authorities process personal data when there is a legal obligation established by EU or Member State law that allows for such processing and meets the conditions outlined in Article 6(1)(c) and Article 9(2)(i) of the GDPR¹²²⁰. Any national law must include specific and appropriate measures to safeguard the rights and freedoms of data subjects. Generally, the more significant the impact on individuals' freedoms, more solid corresponding measures ought to be provided in the relevant law. Existing EU and Member State laws before the COVID-19 outbreak, as well as those being enacted to combat the spread of epidemics, may serve as a legal basis for processing individuals' data if they permit epidemic monitoring and meet additional requirements stated in Article 6(3) of the GDPR.¹²²¹ Remaining reliant on the law as the legal basis contributes to legal certainty considering the nature of the personal data involved, especially health data, and the circumstances of the current pandemic. However, it is important to recall what is set out by the EDPB that the data processing should also be proportionate to the intended purpose, ensuring that it is necessary and does not disproportionately infringe upon

¹²¹⁸ See article 7 of the GDPR, conditions for consent.

¹²¹⁹ EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679, *op.cit.*, p.17.

¹²²⁰ These references made to the GDPR articles respectively set out the processing of personal data and processing of special categories of personal data.

¹²²¹ Guidance to ensure full data protection, *op.cit.*, p.2.

individuals' privacy.¹²²² Therefore, from our point of view, as a positive act towards this direction, the Guidance elaborated that such reliance ensures that the processing of specific health data is prescribed in detail, specifies the purposes of processing, clearly identifies the controller (the entity processing the data) and others with access to the data, prohibits processing for purposes other than those enlisted in the legislation, and provides particular safeguards.¹²²³

Having said that, although these are positive due to their privacy-friendly nature, we still believe that the limits of lawful basis was left vague in the recommendation, on contrary to the general recommendation of the EDPB¹²²⁴. In other words, considering that now, the temptation to “do whatever it takes” for the success of the applications is huge¹²²⁵, we believe that there should be the limit on derogations from data protection rights, even in the most urgent circumstances, which must be underpinned by the Commission guidelines in particular. Undoubtedly, a crisis will increase the need for governments to monitor and control their citizens, and may require restrictions on individual liberties, and such decisiveness is characteristic of many emergencies.¹²²⁶ To be more specific, for instance, the EDPB published the Guideline on Restrictions under Art. 23 GDPR¹²²⁷. Regarding the right of access, the EDPB reminds controllers to remove limitations as soon as the justifications for them cease to exist.¹²²⁸ The reason is that there is always the

¹²²² Guidance to ensure full data protection, *op.cit.*, p.2.

¹²²³ Guidance to ensure full data protection, *op.cit.*, p.3.

¹²²⁴ For the detailed guidance see EDPB (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p.15 and p.16.

¹²²⁵ Zwitter, Andrej and Gstrein, Oskar Josef (2020) "Big data, privacy and COVID-19—learning from humanitarian expertise in data protection", *Journal of International Humanitarian Action*, vol. 5, no. 1, pp. 1-7, p.2.

¹²²⁶ Zwitter, Andrej and Gstrein, Oskar Josef (2020) "Big data, privacy and COVID-19...", *op.cit.*, p.2.

¹²²⁷ For the full guidance see EDPB (2020) Guidelines 10/2020 on Restrictions under Art. 23 GDPR.

¹²²⁸ EDPB (2023) Guidelines 01/2022 on data subject rights - Right of access, p.57.

risk of trigger of the Article 23 of the GDPR,¹²²⁹ which establish legal basis of restriction on content of the obligations and rights provided to data subjects. Particularly, such considering that public interest was listed one of the valid reasons of such restrictions on data subject rights.¹²³⁰ Therefore, we are of the view that, it is crucial to delineate the limits of the lawful basis as well as restrictions applied on data subject rights going forward. Having said that, it is worth mentioning that none of the data controller did not even stipulate or articulate any potential use of derogations from data protection rights of the individuals based on their policies, notices, and website documents, which is in line with the targeted European approach¹²³¹ for championing data protection law and data subject rights.

Subsequently, regarding data minimization practices, the EU guidance set out something different than other counterparts by both pointing out the ePrivacy Directive¹²³², rather than the GDPR, which we find a bit contradicting with the previous perspectives brought by the EDPB¹²³³ and the Commission¹²³⁴, and differentiate between the different app functionalities that involve various levels of personal data processing. The Guidance set out that an information-only app does not require processing individuals' health data and should only process information necessary to fulfil its purpose. However, if the app includes symptom checking or telemedicine functionalities, personal health data may be processed, and the underlying legislation being applicable to health authorities must specify the data that can be processed. Additionally,

¹²²⁹ See Article 23 of the GDPR, restrictions.

¹²³⁰ Article 23-e sets out that "...other important objectives of general public interest of the Union or of a Member State, in particular ..., public health and social security;"

¹²³¹ For further details on the European approach on data protection law see European Commission, Data Protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 15 July 2023).

¹²³² ePrivacy Directive sets out that "systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum".

¹²³³ It refers to EDPB (2020) Guidelines 04/2020 on the use of location data and contact tracing.

¹²³⁴ It refers to eHealth Network (2020), Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States.

health authorities could require phone numbers of data subjects/users, who have utilized the symptom checker capability and therefore uploaded their results.

Nevertheless, as per the Guidance, processing information stored on the user's device should be limited to what is necessary for the app's functioning and purpose. Accordingly, it is reiterated by the Guidance that location data is unnecessary for contact tracing and can raise concerns regarding data minimization, security, and privacy.¹²³⁵ For instance, the generation and processing of proximity data should occur solely in instances where there exists an actual risk of infection, determined by the closeness and duration of contact between individuals. This is a pro-active approach provided towards use of minimum data possible, in line with the GDPR principles.¹²³⁶ To be more specific, as detailed by the EDPB on data minimization practices in general, the controller must pre-determine which functions and parameters of processing systems and their supporting functions are allowed.¹²³⁷ Accordingly, to decide on the amount of data should be necessary, data minimization demonstrates the principle of necessity and makes it operational.¹²³⁸ To this end, the Guidance associated with the processing of some personal data with consent for different functions. For example, storing the exact time or place of contact is generally not necessary, but knowing the day of contact can help determine if it occurred when the person developed symptoms or 48 hours prior. The choice of the approach for warning close contacts can be either decentralized processing through the app or using arbitrary temporary identifiers stored on a backend server controlled by health authorities. In the latter case, direct user identification through the data is not possible. Therefore, in case health authorities aspiring to contact close contacts by phone or text messages, they require data subject consent to be

¹²³⁵ Guidance to ensure full data protection, *op.cit.*, p.4.

¹²³⁶ See Article 5-1-c of the GDPR, data minimisation.

¹²³⁷ EDPB, (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, p.21.

¹²³⁸ *Ibid.*

provided with their phone numbers. Having said that, the document in favour of the decentralized solution as it aligns better with the principle of data minimization anyway.

From data controller perspective, we believe that this is positive but cumbersome for the implementation of detailed approach on the consent and the type of the data processed, which differs from the other guidelines analysed in this Chapter. Additionally, this is in line with the perspective we provided in Chapter 3 and 4 on detailed and transparent approach regarding the type of personal data processed, and implementation of the informed consent of the data subject users. Accordingly, from our perspective, as the positive side of this approach, some data controllers as detailed in Chapter 3, created this bridge between the different functionalities and efficient data protection law safeguards such as elaborate consent for different type of features. As detailed in Chapter 1, many of the data controllers implemented elaborated approach against the different use of personal data of the users. They did not simply indicate the type of personal data used. On the contrary, for instance, Austrian¹²³⁹, French¹²⁴⁰, German¹²⁴¹, Irish,¹²⁴² and Latvian¹²⁴³ apps were designed to implement different amounts of data processing and different level of consent requirement for each type of processing for instance for processing to obtain lab results data¹²⁴⁴, or processing for accessing EU Digital certificate, or data processed when withdrawing an infection report provided by the doctor, etc. On the concerning side of such approach, as detailed in Chapter 3 that, implementing consent could be quite difficult to manage for data controllers for each specific type of personal data processed.

¹²³⁹ See Stopp Corona Application, op.cit., Section 4.

¹²⁴⁰ See Tous Anti-Covid Privacy, op.cit., Legal Basis and Regulatory Nature of the Processing Section.

¹²⁴¹ See Corona Warn, Privacy, op.cit., Section 2 and 3.

¹²⁴² See Corona Alert, Privacy Statement, op.cit., Section 4.

¹²⁴³ See Korona Stop Application Privacy Policy, op.cit., Section 5.

¹²⁴⁴ See Corona Alert, Privacy Statement, op.cit., Section 3, para 1.

Mentioning of using differing among functionalities by the Guidance, the purposes of the apps are elaborated in the Guidance¹²⁴⁵ as follows:

- Information functionality: The purpose is to provide relevant information from the health authorities in the scope of the crisis.
- Symptom checker and telemedicine functionalities: The purpose is to assess symptoms or provide medical advice related to COVID-19.
- Contact tracing and warning functionalities: The purpose is to retain contacts of app users who may have been exposed to COVID-19 infection -in order to warn potentially infected individuals and prevent further infections.

For instance, regarding the limitation of data disclosure and access, no data stored on and accessed from the user's device for the information functionality can be shared with health authorities beyond what is necessary for the functionality itself.¹²⁴⁶ This means that health authorities will not have access to any other data besides the information functionality. For the symptom checker and telemedicine functionalities, it may be determined that responsible health authorities and national epidemiological authorities should have access to the information provided by the patient. For instance, only the European Centre for Disease Prevention and Control (ECDC) could receive aggregated data from national authorities for epidemiological surveillance.¹²⁴⁷

Therefore, we are of the view that indication of the different functionalities and purposes of processing are also remarkable difference from the other guidance, and potentially even shaped the attitude of data controller authorities to contemplate the relationship between functionality and legal purpose of data processing activities. As also mentioned by ICO guidance that despite the potential benefits that additional functionality may have for helping medical professionals fight for pandemic, any additional functions or

¹²⁴⁵ Communication from the Commission, *op.cit.*, p.4.

¹²⁴⁶ Communication from the Commission, *op.cit.*, p.4.

¹²⁴⁷ ECDC (2020), Mobile applications in support of contact tracing for COVID-19 A guidance for EU/EEA Member States, p.1.

features must be evaluated on a case-by-case basis.¹²⁴⁸ Accordingly, each data controller's privacy policy detailed in Chapter 1 seemed to try to indicate the same approach, as they provided elaborate mechanism to indicate the purpose of processing for each specific case-scenarios, which we find in line with the European approach on the data protection matters holistically¹²⁴⁹. Correspondingly, the Guidance advised against bundling different functionalities together to provide individuals with more control over their data. Should there arise a necessity for objectives like scientific research and statistical analysis, they ought to be explicitly included in the original list of purposes and distinctly communicated to users¹²⁵⁰, which we strongly concur, from the perspective of optimal transparency and rule of law.

Furthermore, we also believe that it is possible to observe this distinction for the retention mandates of the data controllers, which we always find it in bit of contradiction with the processing non-identified data at stake, given that lack of explanation on the type of the processing data, merely stating the importance of limited retention was raising question marks in the eyes of the data subject users. Therefore, in line with the approach proposed in Chapter 4, with regards to the processing of unidentifiable data, it is also satisfying to observe detailed and distinguished approach. To get back to the distinction provided by the guidance, they classified that the timelines for data retention should be determined based on medical relevance (such as the incubation period) and realistic durations for administrative procedures.

Additionally, we find promising to observe the importance of the deletion of any sort of processed data, which we proposed in Chapter 3, was detailed by setting out that data processed within the scope of the Information functionality purposes, any data collected during the installation of this

¹²⁴⁸ ICO guidance COVID-19 Contact tracing: data protection expectations on app development *op.cit.* p.2.

¹²⁴⁹ For further details on the European approach on data protection law see European Commission, Data Protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 15 July 2023).

¹²⁵⁰ Communication from the Commission, *op.cit.*, p.4.

functionality should be promptly deleted as there is no valid reason to retain such data.¹²⁵¹ It is even more elaborate and privacy friendly in comparisons with what other guidance indicates, as the Guidance differentiated the deletion regimes data controllers subject to, as per the functionality of processing activity,¹²⁵² which believe is certainly in line with the general approach brought by EDPS which set out when the epidemic has ended and contact tracing apps are no longer required, a protocol should be established to halt the collection of identifiers, which could comprise globally deactivating the application and deleting all collected data from all databases, including those on mobile applications and servers.¹²⁵³

To be more concrete, for instance, for the symptom checker and telemedicine functionalities, the guidance set out that health authorities should delete such data after a maximum period of one month (incubation period plus margin) or if the person tests negative. However, health authorities may retain data for longer periods if it is anonymized and used for surveillance reporting and research purposes. Ultimately, proximity data used for contact tracing and warning purposes should be deleted once it is no longer needed to notify individuals. However, health authorities can retain anonymized proximity data for extended periods in case it is utilized for surveillance reporting and research. The data should be stored on the user's device, and only the necessary data communicated by users should be uploaded to the server accessible to health authorities (e.g., uploading data of "close contacts" of a person who tested positive for COVID-19). To this end, as per our assessment, most of the data controllers, including but not limited to

¹²⁵¹ Communication from the Commission, *op.cit.*, p.9

¹²⁵² *Ibid.*, p.9.

¹²⁵³ EDPS (2020), TechDispatch #1/2020: Contact Tracing with Mobile Applications, Purpose Limitations Section, https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en (accessed on 23 June 2024).

French¹²⁵⁴, Dutch¹²⁵⁵, Italian¹²⁵⁶, Austrian¹²⁵⁷ and German¹²⁵⁸ authorities, indicated a very much detailed approach on the use of limited retention period for the different set of data processed for the varied features of the applications, or retrospective upload of the data. Hence, we are of the view that again the privacy-friendly approach of the Commission steered a privacy-friendly situation for the compliance activities of the data controllers, which means that the target is accomplished on a high-level.

Subsequently, regarding the accuracy of the personal data at stake, to safeguard data, the description of ensuring the accuracy of the personal data being processed is clear enough to delineate the importance of the keeping data accurate and up to date in line with the GDPR requirements¹²⁵⁹. That is to say, the Commission stated that it is essential to accurately determine whether a contact has occurred between an individual and an infected person in terms of epidemiological distance and duration to minimize the risk of false positives.¹²⁶⁰ This consideration applies to scenarios where app users come into contact on the street, in public transportation, or within a building. Relying solely on location data from mobile phone networks may not provide sufficient accuracy for this purpose. Therefore, the Guidance seems to follow the same path as other counterparts is recommended to utilize technologies, such as using Bluetooth, which enable a more precise assessment of contact. Furthermore, as also discussed by Williams and colleagues and separately detailed in Chapter 2 with instances, there might be certain concerns around

¹²⁵⁴ Tous Anti-Covid Privacy, *op.cit.* Legal Basis and Regulatory Nature of the Processing Section.

¹²⁵⁵ Corona Melder, Privacy Policy, *op.cit.*, Section 7.

¹²⁵⁶ Immuni Application Documentation, *op.cit.*, Section Epidemiological information

¹²⁵⁷ The Stop Corona App, Privacy Policy, Section 6.

¹²⁵⁸ Corona Warn, Privacy, *op.cit.*, Section 9

¹²⁵⁹ See Article 5 of the GDPR, already mentioned.

¹²⁶⁰ Communication from the Commission, *op.cit.*, p.9.

stigma of users, due to privacy and wrong perception related concerns,¹²⁶¹ which we believe might result from the inaccurate data usage.

Having said that, the Commission also recommends storing it in encrypted form on the user's device using advanced cryptographic techniques.¹²⁶² If data is stored on a central server, all access, including administrative access, should be logged.¹²⁶³ This is reflected by the centralized applications such as France and Norwegian and as detailed in Chapter 1. On the other hand, like the other counterparts, the Guidance reiterated that proximity data should only be generated as well as stored on the user's device in an encrypted and pseudonymized format. Temporary user IDs which regularly changes are preferable for collecting proximity data via Bluetooth Low Energy (BLE) instead of retaining genuine device ID, as this enhances defence against eavesdropping and tracking by hackers, making it more challenging to identify data subjects.

This approach brought by the Commission is important for the risks associated with Bluetooth data detailed in Chapter 2, which may lead to intrusive data processing activities. Considering that for the purposes of contact tracing, demanding access to personal devices could be more efficient than merely leveraging anonymized mobile positioning data.¹²⁶⁴ Therefore, adding a detail on the temporary user IDs, also done by the Guidelines 04/20 as detailed above, is in line with the tracking and re-identification related risks, and may act as a preventive solution for data controllers. Accordingly, as per their policies and website documents, technical specifications, almost each of the data controllers relying on the BLE opted for the same logic provided by both the Commission and the EDPB for the use of temporary user IDs, which

¹²⁶¹ Williams, Simon N.; Armitage, Christopher J.; Tampe, Tova and Dienes, Kimberly (2021) "Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study", *Health Expect*, vol.24, n.2, pp. 377-385, p.381.

¹²⁶² Communication from the Commission, *op.cit.*, p.9.

¹²⁶³ Guidance to ensure full data protection, *op.cit.*, p.4.

¹²⁶⁴ Ienca, Marcello, and Vayena, Effy (2020) "On the responsible use of digital data to tackle the COVID-19 pandemic." *Nature medicine* 26, no. 4 pp. 463-464, p.464.

certainly is an important step, considering that so far we have not faced with any sort of intrusive act in data protection law related to the re-identification of data subjects.

Notwithstanding, we believe that, as part of the unified approach among EU institutions to uplift privacy during Covid time, it is important to mention the European Parliament's ¹²⁶⁵ act thereon. The EU's concerted action to combat the COVID-19 epidemic and its effects was decided in favour of by the Parliament, who voted in support of a decentralized strategy. ¹²⁶⁶ The Parliament asserts that the data generated should not be stored in centralized databases and such databases pose potential risks of abuse, loss of trust, and may jeopardize the widespread acceptance and adoption of the system across the Union, ¹²⁶⁷ which is in line with the feared events discussed in Chapter 2, and herein as well, to act firmly and jointly against these risks, it is important to implement a cross reference among the institutions' guidelines. Positively, the Guidance also acted in the same manner by pointing out the fact that in establishing national frameworks, legislation should be adopted to ensure that all researchers participate in collaborative research activities under compatible terms and that cross-border cohorts can be efficiently constructed and managed, and the EDPB may act as a coordinator or convener of such processes. ¹²⁶⁸ This is certainly in line with our proposed unity and compatibility approach, and will enable researchers to address not only future pandemics, but other pressing public health priorities.

¹²⁶⁵ See European Parliament, European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (Resolution) (Europe: European Parliament, 2020).

¹²⁶⁶ Ogbuefi, Nnubia (2021) "Contact Tracing and Its Approach to Privacy Under Europe and Canada's Privacy Laws", Available at SSRN 4248282, pp.1-59, p.26.

¹²⁶⁷ *Ibid.*

¹²⁶⁸ Guidance to ensure full data protection, *op.cit.*, p.3.

Within the same remit, also, the Commission delineated certain organisational measures¹²⁶⁹, which suggests making the app's source code available for public review.¹²⁷⁰ Further measures, such as auto-deletion or anonymization of data after a specific time period, can be performed to secure the processed data, which we believe is both in line with the aforementioned limited data retention perspective as well as the proposed solution from our end on Guidelines 04/20 for the implementing a recurring review mechanism both for the guideline and data controllers to stay up-to-date against unexpected data protection law related changes. Or similarly, with regards to involving Data Protection Authorities to the process, the Guidance set forth that Data Protection Authorities should be actively engaged and consulted during the development of the app, and they should oversee its deployment.¹²⁷¹ Since the processing of data within the app involves handling a large volume of special categories of data (health data), the Commission highlights the importance of complying with Article 35 of the GDPR¹²⁷², which pertains to conducting a data protection impact assessment.

As a remarkable aspect provided by the Recommendation, the Guidance encourages establishing independent oversight mechanisms and accountability measures to ensure compliance with data protection standards. This can include appointing data protection officers, conducting privacy impact assessments, and involving data protection authorities in the design and implementation of contact tracing apps. It created more realistic and cutting-edge solution for the data controllers, given that such dynamic approach are mostly preferred by private companies or organisations to

¹²⁶⁹ As per the article of Elisavet Dravalou (2021) (mentioned already) internal policies, organizational standards, controls, and audits are a few examples of organizational measures that controllers and processors might use to guarantee the protection of personal data, which could assist in maintaining uniformity in the protection of personal data across the whole processing cycle, available at: <https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/> (accessed on 22 June 2024).

¹²⁷⁰ Guidance to ensure full data protection *op.cit.*, p.4.

¹²⁷¹ Guidance to ensure full data protection *op.cit.*, p.4.

¹²⁷² See Article 35 of the GDPR, data protection impact assessment.

response quickly to any sort of unexpected data protection breaches, as we detailed in Chapter 3, in order to mitigate such dynamic risks around data protection law. Particularly, we believe that to go one step further from the point set by the Commission recommendation, we can even provide that the Commission would provide the nuances of incident response plans in the DPIA recommended, nuances of the privacy-by-design and default processes, the role and accountabilities of data protection officer, rather than relying on the GDPR requirements for these matters merely, as described in previous sections, a fine-tuning is required for the application of these general GDPR requirements due to the uniqueness of pandemic events. Having said that, although there are aforementioned matters that need to be enhanced from the regulatory perspective for any potential future case scenario, the approach brought by the Commission is still valid, particularly when we consider the holistic view of the EU data protection actors¹²⁷³ and their analysed guidelines, the role of the guidance issued by the Commission is significant as well. Correspondingly, it is plausible to state that data controllers seemed to be positively impacted by these good-purpose acts with regards to their emphasize on privacy-by-design, but for the DPIA and data protection officer selections there seems to be further work needs to be done, as detailed in Chapter 3 and 4 as well.

4. Commission Recommendation (EU) 2020/518 Of 8 April 2020 On A Common Union Toolbox For The Use Of Technology And Data To Combat And Exit From The COVID-19 Crisis, In Particular Concerning Mobile Applications And The Use Of Anonymized Mobility Data

On 8 April 2020, the European Commission adopted the Communication from the Commission Guidance on Apps supporting the fight against Covid 19

¹²⁷³ With this reference, we referred to EDPB, EDPS, EU Commission and National Data Protection Authorities of the Member states. For further details on the European Institutions acting as data protection actors see European Commission, Data Protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 15 July 2023).

pandemic in relation to data protection 2020/C 124 I/01 (European Commission, 2020), establishing nonbinding requirements to ensure app developers comply with EU privacy and personal data protection legislation (GDPR and e-Privacy Directive).¹²⁷⁴ Given the purposes of smartphone applications as stated above, their use may have an impact on how well several fundamental rights, like the right to respect for one's privacy and family life, are exercised. As any interference with those rights must be legal, Member States' laws that would specify or authorize restrictions on the exercise of fundamental rights must be compliant with their constitutional traditions, international legal obligations, and the general principles of Union law set forth in Article 6 of the Treaty¹²⁷⁵ on the European Union.¹²⁷⁶

Accordingly, the Guidance set out that at the outset processing of health data must be governed as per the GDPR principles, and such data may be processed, among other things, once a data subject provides their explicit consent or when processing is necessary for purposes of monitoring and alerting, the prevention or control of communicable diseases, or other serious health threats, as defined by Member State or Union law.¹²⁷⁷ Therefore, the guidance did not differ from the previously analysed guidance in terms of reference to the GDPR, as it should be. Nevertheless, we are of the view that, as a minor difference, it specifies and prioritizes the importance of consent, since it was provided accordingly in the GDPR.¹²⁷⁸

Having said, it also pointed out a way out for controllers of the consent requirement of the GDPR, by indicating that number of Member States have

¹²⁷⁴ Newlands, Gemma; Lutz, Christoph; Tamò-Larrieux, Aurelia; Fosch Villaronga, Eduard; Harasgama, Rehana and Scheitlin, Gil (2020) "Innovation under pressure: Implications for data privacy during the Covid-19 pandemic", *Big Data & Society*, vol. 7, no. 2, 2053951720976680, pp.1-14, p.10.

¹²⁷⁵ See Article 6 of the Treaty on European Union.

¹²⁷⁶ Commission Guidance on Apps., op. cit. p.4.

¹²⁷⁷ Commission Guidance on Apps., op. cit. p.2.

¹²⁷⁸ See article 9 of the GDPR, already mentioned.

passed particular legislation (Articles 6(1)(c)¹²⁷⁹ or (e) and Article 9(2)(i) of Regulation (EU) 2016/679) that permits them to process health data based on public interest.¹²⁸⁰ What data are to be processed and by whom should all be made plain and explicit along with the aims and methods of the data processing. While, as also described in the previous section that each of the data controllers specified in detail the nature of the processing activities, methodology of processing activities, and type of data processed explicitly, still, we are not convinced that, as analysed in the previous Chapters, consent-based approach is not creating best practice from the data protection perspective. Therefore, implementing lawful basis as detailed in Chapter 3 is more in line with the reality of the life, in contrary to previous section of this Chapter. On the other hand, in case consent is not chosen by data controllers, there are certain checks and balance mechanism are provided by the Commission too, in order to prevent any sort of feared or abusive event that could take place with regards to the arbitrariness of the controllers in processing activities, which we find more of added-value to the activities on data controller, given that each of them rely on public health lawful basis for their processing activities.

Subsequently, we are of the view that the Guidance touch based on three significant matters for the entire picture of data protection matters, which would create both successful sample for the future uses of the applications in different pandemic scenarios and create bit of controversy going forward. Correspondingly, the first one is, an affirmative act to keep the dialogue among important data protection law actors in the European law. Accordingly, the Guidance stated that the Commission can consult EDPS and the EDPB, in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council (4) and Article 70 of Regulation (EU)

¹²⁷⁹ Article 6-1-c- of the GDPR oversees the requirements to be met for the processing of personal data, whereas Article 9(2)(i) of the GDPR enshrines the requirements for the processing of special categories of personal data, as already mentioned.

¹²⁸⁰ Commission Guidance on Apps., op. cit., p.2.

2016/679,¹²⁸¹ which believe opened the gates of further alienation between these stakeholders, which would result in less room for the intrusive data processing activities from the legal perspective. Secondly, the Guidance stated that the rules governing traffic and location data, as well as the keeping of information and getting access to information held in a user's or subscriber's terminal equipment, such as a mobile device, are outlined in Directive 2002/58/EC of the European Parliament and of the Council.¹²⁸² According to Article 5(3)¹²⁸³ of the Directive, such storage or access is only permitted under specific conditions or with the user's or subscriber's consent after being given full and clear disclosure in accordance with Regulation (EU) 2016/679 requirements.¹²⁸⁴ Additionally, Article 15 (1) of the Directive permits Member States to adopt legislative measures to limit the application of some rights and obligations outlined in the Directive¹²⁸⁵, including those in Article 5, when such a restriction is necessary, fitting, and proportionate within a democratic society to accomplish particular objectives.¹²⁸⁶

Last of the points, which we find crucial, it referred to another Commission communication on "European Strategy on Data",¹²⁸⁷ permitting the flow of data within the EU and across sectors for the collective benefit of all involved and the creation of a single market. Given that data protection laws are fully respected, and the rules for data access and use are fair, practical and clear across the EEA, the committee said it would consider the need for legislative action to facilitate data sharing between businesses and

¹²⁸¹ Commission Guidance on Apps., op. cit., p.2.

¹²⁸² Commission Guidance on Apps., op. cit., p.3.

¹²⁸³ For the full definition see Article 5 of the GDPR, already mentioned.

¹²⁸⁴ For the full details see Article 5(3) of the ePrivacy Directive.

¹²⁸⁵ For the full details see Article 15 (1) of the ePrivacy Directive.

¹²⁸⁶ Commission Guidance on Apps., op. cit. p.4.

¹²⁸⁷ Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A European Strategy For Data available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066> (accessed on 23 June 2024).

governments for the public good.¹²⁸⁸ Accordingly, from our angle, the emphasize on data flow is of great importance for the implementation of interoperability matters as well. Considering that gateway initiative created for the interoperable implementation of data sharing among the apps,¹²⁸⁹ such approach on the free flow of data provided by the Guidance opened the door for interoperable approach as well, which will be elaborated in the next section. Even though it did not directly impact the decision of controllers, we consider this as an important thing to mention, as the emphasis on data flow between member states reminded of what is being targeted by member countries for many years, which should not be any difference during pandemic period too. We, therefore, believe that sometimes regulators point out one direction even with one simple sentence, and such perspective could radically impact the way both controllers and authorities operate, which is exactly the case in this sample as well.

On the other hand, interestingly, it might be deemed as a sort of confession that the Guidance provided that the ongoing crisis highlights the advantage for health authorities and research institutions in having increased access to vital information to study virus progression and evaluate the impact of public health measures.¹²⁹⁰ Accordingly, we have detailed in Chapter 2 the potential risks associated with the large surveillance, but to provide the further details of the greater access delineated the Recommendation, it is worth mentioning particularly for the central data processing activities that the central service infrastructure and this data may be useful for studying and controlling epidemics, but they may also enable extensive behaviour surveillance. To be more concrete, a single point of failure exists with the service, which means that users cannot register or even continue tracing without it.¹²⁹¹ Therefore, as

¹²⁸⁸ Commission Guidance on Apps., op. cit. p.4.

¹²⁸⁹ Gateway Initiative available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904 (accessed on 23 June 2024).

¹²⁹⁰ Commission Guidance on Apps., op. cit., p.4.

¹²⁹¹ EDPS (2020), TechDispatch #1/2020: Contact Tracing with Mobile Applications, available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en (accessed on 23 June 2024).

supported by TechDispatch of the EDPS, in order to establish user trust, such a service must incorporate extraordinary organizational and technological data protection and cyber security precautions¹²⁹², which are reiterated by the other guidelines detailed in this chapter, which are compatible with each other in this respect. In addition to this, the Guidance pointed out the importance of the caveat provided by the World Health Organization ¹²⁹³ and other organizations, by stating that WHO have additionally cautioned about the possibility that applications and erroneous data may lead to the stigmatization of people who share particular features because of a perceived connection with the disease.¹²⁹⁴ As a remediation of such stigma, data controllers are reminded of data minimization practices by the Guidance, and recommended certain techniques such as data availability, authenticity, integrity, and confidentiality must be protected using effective cybersecurity and data security methods.¹²⁹⁵ Although whose details was only provided efficiently in Toolbox, as mentioned in the relevant section of this Chapter, since majority of the data controllers seem to take their stance in accordance with the Toolbox's descriptive guidance for the nuances and necessities of these technical, legal and cyber safeguards.

However, of course, as controllers are potentially being impacted by many different source of the European data protection law, there is a good chance that the call from the Guidance for having explicit and precise processing purpose; ensure data security and accuracy; implement strict data disclosure, access and storage limitation; and use the data minimization principle, ¹²⁹⁶

¹²⁹² EDPS (2020), TechDispatch #1/2020: Contact Tracing with Mobile Applications, available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en (accessed on 23 June 2024).

¹²⁹³ World Health Organization, (2021) "Contact tracing in the context of COVID-19, interim guidance" available at: https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y (accessed on 23 June 2024), p.1.

¹²⁹⁴ Commission Guidance on Apps., op. cit., p.5.

¹²⁹⁵ Commission Guidance on Apps., op. cit., p.5.

¹²⁹⁶ Newlands, Gemma; Lutz, Christoph; Tamò-Larrieux, Aurelia; Fosch Villaronga, Eduard; Harasgama, Rehana and Scheitlin, Gil (2020) "Innovation under pressure...", op.cit., p.10.

could be impactful on the indicative actions of data controllers for the technical and legal measures as detailed in previous sections.

With regards to the legal perspective, as a legitimate basis for data processing, the European Commission reminds that respective article of the GDPR¹²⁹⁷ and the ePrivacy Directive¹²⁹⁸ requires the consent of the user to store or gain access to information already stored on the user's device, unless the storage is necessary for the app, and the user has explicitly requested it. From our perspective, it is plausible to state that the emphasize brought by the Guidance on accuracy of personal data and its potential privacy law impact would be satisfying in terms of reminding data controllers to take necessary steps against implementing anonymized but still inaccurate data, which would lead to stigmatise as also described in Chapter 2. Therefore, even though it was quite succinct and on a high-level, we still believe that such reminder could play an important role in the compliance activities of the controllers, which we also observed in their policies the similar attitude accordingly. On the other hand, significance attributed to cyber security and data minimization measures, are undetailed, in comparison with the other guidance analysed in this Chapter, such as Toolbox. Therefore, we believe that, the nature of the Guidance is a bit different than the other counterparts, due to both its target to trigger a more detailed Toolbox, which we have analysed in this Chapter as well, and providing an emphasis on the importance of multiple stakeholder activity, or in other words collaboration among main actors of the EU for data protection law for the implementation of the data protection measures of these applications.

Furthermore, pertaining to the nuances of the data protection law aspects of the mobile applications, the Guidance set out a list of requirements, to delineate the minimum expectations regarding the data protection compliance activities of data controllers.¹²⁹⁹ These principles can be outlined as follows:

¹²⁹⁷ See Article 6 of the GDPR, lawfulness of processing.

¹²⁹⁸ See Article 5-e of the ePrivacy Directive, confidentiality of communications.

¹²⁹⁹ Commission Guidance on Apps., op. cit., p.4.

prioritizing the least intrusive yet effective measures, such as using proximity data while avoiding the processing of detailed location or movement data, and employing anonymized and aggregated data whenever feasible; implementing safeguards to uphold fundamental rights, specifically adhering to regulations on personal data protection and communication confidentiality, ensuring data is stored on mobile devices, and managing potential access by health authorities.¹³⁰⁰ Correspondingly, we are of the view that, most of these expectations, again, are compatible with the other requirements put forward by the guidelines/guidance analysed in this Chapter, therefore, it played its complementary role thoroughly, and they are predominantly considered by the data controllers for the design and implementation of their applications, based on their privacy policies, technical specifications, and terms and conditions documentations.

Nevertheless, most importantly, the Guidance sets forth the termination of implemented measures and the deletion of personal data collected through these measures once they are no longer deemed necessary.¹³⁰¹ Accordingly, we consider, as the most notable difference from the other guidelines, pointing out the expiration of the measures implemented by data controllers as per the GDPR¹³⁰², is useful to display the importance of finish line of the controller's responsibilities, which we believe that not many guidance or scholar elaborated this approach. In other words, so far, we have noticed that most of the discussions, counter arguments and hypothesis have been scattered around the vulnerability of data subject and potential detrimental impact of the acts that could be taken by data controllers. We understand this is the most controversial and crucial one due to the importance of fundamental privacy rights¹³⁰³. On the other hand, from our perspective, it might also create unfair circumstance, if none of the regulators nor scholars point out the balance to

¹³⁰⁰ Commission Guidance on Apps., op. cit. p.4.

¹³⁰¹ Commission Guidance on Apps., op. cit. p.4.

¹³⁰² See Article 32 of the GDPR, security of processing.

¹³⁰³ In this reference, we referred to data subject rights provided in the GDPR between article 12 to 23.

be stroke between the liability of data controllers and data subjects' rights. Therefore, even though it is a high-level touch by the Commission on the topic, it is still important to observe the mention of finish end for the hard work of data controllers as well.

This might create a great response for the circumstances in which data controllers are assigned many tasks, but the ending point were not really specified. For instance, to provide greater specificity, the perspective articulated by ECDC¹³⁰⁴, underscores the imperative involvement of public health authorities across all stages: from app selection, development, piloting, deployment, to evaluation. This active engagement ensures optimal public health protection while duly prioritizing concerns regarding privacy and data protection,¹³⁰⁵ could be an important indication of such approach we are discussing right now. Going forward, it would be an efficient move to detail the boundaries of the data controllers as well, which seem to be not delineated by the EDPB for other processing activities, from this perspective.¹³⁰⁶ Within the same vein, as also outlined in the Vinuesa et al. study, the EDPB guidelines include a provision to stop using the app once the situation is "normal" again.¹³⁰⁷ This can be seen as vague, because the word "normal" is open to interpretation given the socio-economic changes that lockdowns have brought. A clearer date would be preferable unless further action is taken.¹³⁰⁸ Correspondingly, sunset clauses offered by the European Parliament resolution for the apps, which basically provide that the apps ought to contain

¹³⁰⁴ For the full document see ECDC (2020), Mobile applications in support of contact tracing for COVID-19 A guidance for EU/EEA Member States,

¹³⁰⁵ ECDC (2020), Mobile applications in support of contact tracing for COVID-19 A guidance for EU/EEA Member States, p.1.

¹³⁰⁶ For the further information see EDPB (2021) Guidelines 07/2020 on the concepts of controller and processor in the GDPR https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en (accessed on 23 June 2024).

¹³⁰⁷ Vinuesa, Ricardo; Theodorou, Andreas; Battaglini, Manuela and Dignum, Virginia (2020) "A socio-technical framework for digital contact tracing", *Results in Engineering*, vol. 8, 100163, pp.1-4, p.2.

¹³⁰⁸ Vinuesa, Ricardo; Theodorou, Andreas; Battaglini, Manuela and Dignum, Virginia (2020) "A socio-technical framework ...", *op.cit.*, p.2.

sunset clauses to ensure that they will not be utilized when the pandemic is over,¹³⁰⁹ which we strongly find as efficient to tool to mitigate any dependency on both parties of the processing activities.

Nevertheless, apart from this matter, we believe that given the relatively shorter nature of the document itself, it still touched diverse and important points, which must be addressed by data controllers on a high-level in conjunction with other guidelines detailed here. For instance, despite the criticisms on even the most criticized applications, such as Norwegian, French, Portugal and Lithuanian for some features of their applications' processing activities, it is still privacy-friendly approach to delineate point of contact for any data protection matters that could arise following the removal of the application, as recommended by the document, which we believe indicates the contribution of the document somehow. That being said, we should also reiterate there were also some controllers they did not specify point of contact or designated person for the data protection queries, as detailed in previous Chapters. Hence, it is not possible to state that there are many outstanding approaches were extracted from this communication. Therefore, realistically speaking, the contribution of this guidance could be more visible once it is considered in conjunction with other guidelines analysed in this chapter from more holistic view.

5. Interoperability Guidelines EU

For many years, interoperability has been a significant problem in healthcare information systems.¹³¹⁰ While some progress has been made with the definition of specific interoperability standards, a framework that can guarantee full interoperability between various systems has not yet been

¹³⁰⁹ EU coordinated action to combat the COVID-19 pandemic and its consequences European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP), point 52.

¹³¹⁰ Ravizza, Alice; Sternini, Federico; Molinari, Filippo; Santoro, Eugenio and Cabitza, Federico (2021) "A proposal for COVID-19 applications enabling extensive epidemiological studies", *Procedia computer science*, vol.181, pp 589-596, p.592.

released.¹³¹¹ On a high level, it is possible to delineate in accordance with the stringent EU standards on data protection for apps, the proximity information shared between applications would be sent in an encrypted manner that prohibits the identification of a specific person; no geolocation data could be utilized.¹³¹² However, there are many nuances that needs to be discussed for the specifics of the apps.

This section, therefore, outlines the interoperability requirements and discusses the key challenges associated with them. To begin with the term of interoperability within the scope of contact tracing apps, for the purposes of interoperability guideline document, interoperability refers to the ability of these apps to exchange the minimal amount of information required so that specific app users, wherever they may be in the EU, are informed if they have been in close proximity to another user who has informed the app that they have tested positive for COVID-19 within a relevant time frame.¹³¹³ This warning and any further action taken should follow the protocols established by public health authorities, with any potential privacy and security consequences evaluated and the necessary protections implemented.¹³¹⁴ Nevertheless, it is important to note that EU data transfers in the GDPR is also touching base the matter of interoperability. The eHealth Network and the European Commission worked together to develop guidelines to ensure interoperability between these apps¹³¹⁵. Therefore, the interoperability matter is not directly overseen by a single guideline, in contrary to the guidelines. We will analyse the interoperability related parts of the respective guidelines and

¹³¹¹ Ravizza, Alice; Sternini, Federico; Molinari, Filippo; Santoro, Eugenio and Cabitza, Federico (2021) "A proposal for COVID-19 ..." op.cit., p.592.

¹³¹² See European Commission, Interoperability https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043 (accessed on 23 June 2024).

¹³¹³ eHealth Network (2020) Interoperability guidelines for approved contact tracing mobile applications in the EU, p.3.

¹³¹⁴ *Ibid.*

¹³¹⁵ For the full guidance see eHealth Network (2020), Interoperability guidelines for approved contact tracing mobile applications in the EU https://health.ec.europa.eu/system/files/2020-05/contacttracing_mobileapps_guidelines_en_2.pdf (accessed on 23 June 2024).

guidance to come up with the most efficient assessment regarding the implementation of interoperability nuances.

Correspondingly, the guidance provided by the European Centre for Disease Prevention and Control sets out certain considerations that needs to be addressed by the data controller health authorities.¹³¹⁶ First actor that steps in is proximity detection, which corresponds that devices should regularly scan for and broadcast Bluetooth beacons. When two devices come into proximity, the beacon of the other device should be securely recorded and stored. The Bluetooth beacon should contain a privacy-preserving unique identifier that is compatible with different approved apps.¹³¹⁷ Therefore, to proceed with the same logic, the Commission built up a gateway service, an interface to effectively receive and transmit pertinent data from national contact tracing servers and applications, to assist further system simplification, by minimizing the quantity of data sent, consumers' data usage could decrease.¹³¹⁸ Another considering that comes into play for interoperability of the apps is Infection confirmation, which basically means that if a user who is traveling across borders tests positive for COVID-19, the competent authority should provide an interoperable and timely mechanism to allow the user to confirm their infection in their app. A trusted and secure mechanism should be used for communication of COVID-19 test results between national health authorities, ensuring the protection of personal data.¹³¹⁹ Once the infection is officially confirmed, the app should be able to provide relevant information about proximity encounters.

The last element of the ECDC guidance is cross-border transmission chains, which refers that solutions should allow the servers of different Member States to communicate and exchange relevant keys through a trusted and secure

¹³¹⁶ For the full guidance see the guidance provided by the European Centre for Disease Prevention and Control, <https://www.ecdc.europa.eu/en/publications-data/guidance> (accessed on 23 June 2024).

¹³¹⁷ *Ibid.*

¹³¹⁸ See European Commission Website, Interoperability https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043 (accessed on 23 June 2024).

¹³¹⁹ See the guidance provided by the European Centre for Disease Prevention and Control, *op.cit.*, p.8.

mechanism. There should be a communication mechanism among Member States to ensure transparent and timely updates regarding any changes in their respective systems.¹³²⁰

Therefore, considering these key elements highlighted above, firstly, it is possible to state that each factor causing vulnerability or risk for the data protection law are determined precisely. For instance, the implementation of data protection law related measures set out in the GDPR and ePrivacy Directive called out clearly from a unified and overarching perspective for the data controllers regarding exchange of the information across the national authorities. In other words, it means for the data controllers that each of the detailed technical and organisational measures both stipulated under the GDPR¹³²¹, and the respective Guidelines must be leveraged to the international aspects of the usage. This is not a straightforward task, obviously, due to various challenges, which will be detailed in the following parts of this section. However, as a good risk-mitigant, from our perspective, employing Bluetooth beacon that contain a privacy-preserving unique identifier is compatible with different approved applications across the member states, and is the most important signal of such approach. Such necessity set out by the EDPC guideline for interoperability matters is certainly being addressed by the joint data controllers of gateway document as well.¹³²² Correspondingly, as per the Gateway document, data controllers could be able to demonstrate their compliance with unified and elaborated approach on technical and organisational measures¹³²³, on which each data controller agreed.

Another significant point addressed by the briefing of the European Parliament ITRE guidance for the interoperability matters, namely third

¹³²⁰ See the guidance provided by the European Centre for Disease Prevention and Control, op.cit., p.8.

¹³²¹ See Article 32 and Recital 78 of the GDPR, already mentioned.

¹³²² See EU Commission, Gateway document, National Joint Controllers and privacy policies https://health.ec.europa.eu/system/files/2023-02/gateway_jointcontrollers_en.pdf (accessed on 23 June 2024).

¹³²³ For the definition see Article 32 of the GDPR, security of processing.

countries' access to the data.¹³²⁴ As indicated by ITRE the main issue with having a variety of national COVID-19 contact tracking applications is not knowing if they will function when citizens of one country visit citizens of another.¹³²⁵ It might become more difficult to use an experimental technology while traveling and might be necessary to try to use components from a typical smartphone for a task for which they were never intended.¹³²⁶ In this regard, the guidance set forth that the interoperability mechanisms mentioned above should be publicly accessible so that third countries can work towards accessing them, subject to security requirements, especially regarding the authenticity of test data. For instance, Denmark data controller, Smittestop, has been part of the European Federation Gateway Service (EFGS). This means that when someone reports themselves as infected in Smittestop your rolling ID's are also uploaded to the EFGS and distributed to the app users of other European contact tracing apps.¹³²⁷ Similarly, the Slovenian application also stated the fact that processed data will be accessible by other countries that are member to Gateway,¹³²⁸ or as per the EU Gateway document, Malta, Ireland, Belgium, Croatia, Italy, Latvia, Czech, Austria, Cyprus, Denmark, Estonia, Spain, the Netherlands, Finland, Norway and German applications were taking part in this initiative to facilitate data flow across the apps.¹³²⁹ This is very much crucial point due to the two reasons; first of all, we find the disclosure of the European residents' data to third countries genuinely crucial due to security reasons, and second of all, the nature of the personal data processed is quite sensitive. Therefore, we do not agree with the perspective

¹³²⁴ See European Parliament Briefing ITRE in Focus, National COVID-19 contact tracing apps, p.2.

¹³²⁵ *Ibid.*

¹³²⁶ *Ibid.*

¹³²⁷ See Denmark Smittestop Privacy Policy, op.cit., Section 7.

¹³²⁸ See Ostani Zdrav, Functioning of the application <https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanizdrav-mobile-application/functioning-of-the-application/> (accessed on 23 June 2024).

¹³²⁹ For the full details of Gateway joint controllers, see EU, National Joint Controllers and privacy policies, https://health.ec.europa.eu/document/download/f2460691-b730-4be5-87d4-474afe09a7fb_en (accessed on 23 June 2024).

brought by the ECDC Guidance document that is supportive of such data sharing with third party controllers. Our reasoning is, not only there have been plenty of discussion around secure countries for data protection law necessities¹³³⁰, but also it might be subject to potential political or commercial use going forward, as detailed in Chapter 2. Hence, our perspective on the issue is that the implementation of technical and organisational measures set out in the appendix of the data transfer clauses¹³³¹ or any similar type of model impacted by this list could be an efficient tool to include in such an arrangement, which is also in line with the general provisions of the GDPR for transfers.¹³³² Obviously, we are aware that it will bring a lot of technical requirement to embed in the process as well. Therefore, from the legal perspective, opening the data at stake to the access of any third countries without elaborate technical and organisational measures evaluated by case-by-case basis, could result in feared intrusive privacy events.

Furthermore, considering that the ECDC guidance set out different apps employ varying algorithms for calculating the risk of exposure it was recommended that information should be shared between apps in a manner that allows for different types of risk calculations.¹³³³ Or similarly, the dates when the proximity encounters took place should be communicated to enable certain apps to consider the timing of exposure in relation to symptom onset or diagnosis and provide appropriate recommendations for quarantine duration if applicable. Therefore, the importance of communication between the member states' authorities as well as the applications are strongly

¹³³⁰ See EU Commission, Secure countries list on the Commission Website under the “Adequacy Decision” available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,Uruguay%20as%20providing%20adequate%20protection. (accessed on 30 June 2023).

¹³³¹ See EU Commission data sharing clauses, also known as “standard contractual clauses” available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on 30 June 2023).

¹³³² See Article 46 of the GDPR, transfers subject to appropriate safeguards.

¹³³³ See the Guidance provided by the European Centre for Disease Prevention and Control.

emphasized by the Guidance.¹³³⁴ On the other hand, from our perspective, the Guidance provided the most important touch on the operationalization of these communication and transparent information target among the member states and data subjects for interoperability of the applications, which we find critical to mitigate the ambiguity due to the language barrier.

To be indicative, as per example provided by the ECDC Guidance that if a citizen and app user from country A (user A) travels to country B and meets a citizen of country B (user B) who later tests positive, user A would receive a notification. In case user A is still in country B at that time, public health authorities need to determine from which country the notification should originate. The simplest approach would be for user A to receive the notification through their own app from country A. This way, the information would be in a language they understand and from a trusted authority. However, it may not provide locally relevant information. Public health authorities could consider collaborating with app developers to customize advice, such as providing a follow-up number specific to the country of visit. We are of the view that this very much crucial part with regards to the proper implementation of privacy notices and notification requirements set out in the GDPR¹³³⁵ and ePrivacy Directive¹³³⁶. Correspondingly, it is very important to set out the recommendations that help controllers to achieve optimal transparency regarding data processing activities targeted by the EDPB¹³³⁷ and the Commission.¹³³⁸ The fundamental challenge is that, whether English is selected for all sort of communication purposes between the apps and data subjects. We believe that it is not realistic to assume that each part of the data

¹³³⁴ See the guidance provided by the European Centre for Disease Prevention and Control.

¹³³⁵ See Article 13 and 14 of the GDPR, already mentioned.

¹³³⁶ See Article 6-(4) of the ePrivacy Directive, already mentioned.

¹³³⁷ For the full information created by EDPB, see EDPB (2018) Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), available at: <https://ec.europa.eu/newsroom/article29/items/622227> (accessed on 2 June 2024).

¹³³⁸ See EDPS Guideline, Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations.

protection law is being implemented without any issues or challenges. From the jurisdictional perspective, it is also unrealistic, as the requirements of transparency may vary across the member states. Still, though, the EDPS emphasized the importance of a single point of contact for the implementation of data subject rights as a consistent transparent information mechanism, not to cause any confusion in the exchange of the information among data controllers and data subjects,¹³³⁹ and the Toolbox indicated well defined procedures at the level of each Member State for how to inform data subjects is required.

Accordingly, as a criticism of the joint controllers, the document of Gateway did not specify any language for the processing activities¹³⁴⁰, which is not in line with the goal of transparency. Therefore, what it could have been provided was that there could be a risk matrix provided for the data controllers using the interoperability service to explain them the significance of multi-language approach, preferable as many as possible, and we believe that in our era, considering the amount of generative AI based tools, it should not be really challenging to diversify the available languages for the data subjects. Hence, we are of the view that considering that it is already risk to engage with implementing multi-jurisdictional data transfers, there should be at least as many legal and technical safeguards as possible to ensure the risk is kept low.

Subsequently, what was described under the Toolbox¹³⁴¹ with regards to the interoperability issues is that first, public health authorities should be obliged to evaluate the effectiveness of the apps at the national and cross-border levels. As per the document, this can be done by cross-referencing contact tracing data with actual test results and assessing the proportion of contacts

¹³³⁹ See EDPS comments on the Commission draft implementing decision amending Implementing Decision 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, p.4.

¹³⁴⁰ EU interoperability gateway for tracing and warning apps available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1905#privacy (accessed on 23 June 2023).

¹³⁴¹ See Toolbox *op.cit.* p.13.

who test positive based on the type of contact exposure. Furthermore, the Toolbox emphasized the importance of effective collaboration and managing cross-border transmission chains.¹³⁴² To this end, it added that national health authorities must have the technical capability to exchange information regarding individuals who are infected with or exposed to COVID-19.¹³⁴³ Likewise, tracing and warning apps should adhere to common EU interoperability protocols to ensure the performance of necessary functions while safeguarding privacy and data protection rights, regardless of the device's location within the EU, which was exactly delineated by the joint controllers as well.¹³⁴⁴ We do not only agree with this view provided by the Toolbox as a main challenge for the interoperable implementation of the apps by data controllers, but also believe that the fact that different nations continue to use different app architectures for their national coronavirus contact tracking would probably a significant factor to increase the complexity of the implementation thereof.

Additionally, the Toolbox also set out that the apps' protocols should be developed and provided to developers, with alignment of epidemiological criteria for defining close contacts in high-risk exposures, based on guidance from the WHO¹³⁴⁵ and ECDC¹³⁴⁶, including the definition of close contact (distance and duration of exposure) and the duration for which contacts are stored. Also, regarding the implementation of interoperability, it mentioned that cross-border data flow between apps relies on consistency between epidemiological frameworks and technical functionalities. Achieving interoperability also requires agreements between national health authorities.

¹³⁴² See Toolbox *op.cit.* p.18.

¹³⁴³ *Ibid.*

¹³⁴⁴ EU Commission, EU interoperability gateway for tracing and warning apps available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1905#privacy (accessed on 23 June 2024).

¹³⁴⁵ WHO, (2020) "Indicator framework for the evaluation of the public health effectiveness of digital proximity tracing solutions" ISBN 978-92-4-002835-7 (electronic version).

¹³⁴⁶ For further information see ECDC (2020), Mobile applications in support of contact tracing for COVID-19 A guidance for EU/EEA Member States.

Hence, the Member States within the eHealth Network, in collaboration with the Health Security Committee and with support from the Commission, should cooperate to define criteria that enable cross-border interoperability to facilitate the collaboration between data controllers of different member states. Based on the practice, the Commission mentioned it is helping Member States find the best solution to ensure secure, protected, and interoperable contact tracing apps across Europe, in accordance with the guidelines provided in the EU toolbox and the Commission's guidance on data protection¹³⁴⁷. Therefore, it created more than a positive approach to include as many member states as possible into the Gateway interoperability initiative.¹³⁴⁸

Having said that, although there is a good atmosphere in terms of the aforementioned collaborative approach, our assessment on the key elements of the framework proposed by the Toolbox is that it did not specify the legal background of the cross-border data processing activities. Particularly, we are of view that, the role of the data transfer regime from the legal perspective is undeniable, considering the data protection risks associated with any sort of cross border data processing activity, which is vastly prevalent in our day. Although this is a low-likelihood assumption, considering the nature of the security among member states for the free flow of data as detailed in Communication from the Commission¹³⁴⁹, we still believe that due to nature of the contact tracing applications, as delineated in Chapter 2, there might be unique or tailored risks arising from the cross-border processing activities. To this end, we strongly are supportive of the view that EU authorities should

¹³⁴⁷ Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU* available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_869 (accessed on 1 July 2023).

¹³⁴⁸ Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU* available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_869 (accessed on 1 July 2023).

¹³⁴⁹ For the full information on security among the member states for data transfers, see Communication From The Commission To The European Parliament And The Council Exchanging And Protecting Personal Data In A Globalised World, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:007:FIN> (accessed on 23 June 2024).

somewhat oblige data controllers to implement transfer impact assessments (TIA)¹³⁵⁰ before engaging with any sort of cross border data transfers, within the scope of interoperable performance of the applications. Such approach for any processing activity is also recommended and supported by EDPS.¹³⁵¹ We also believe that, considering including the existence of a Commission adequacy decision or suitable safeguards, must be given under Art. 13(1)(f) and 14(1)(f),¹³⁵² such obligation must have been reiterated by the Commission on the Recommendation for the use of contact tracing apps. Nevertheless, as also emphasized by the EDPS that most of the documents mainly refer to the GDPR, and for this reason further explanation and details would be needed¹³⁵³. We repeated this necessity also for the other guidelines detailed in this section, including but not limited to interoperability guidelines. Having said that, at the same time, the existence of elaborated DPIA tailored for the interoperability matters, which might have impacted the level of detail provided by the Commission recommendation, given that most matters are covered by the DPIA.

To be more specific, the detailed DPIA made for the interoperability matters¹³⁵⁴ are important indicator of the detailed approach brought by the EU data protection actors on the establishment of detailed risk framework against

¹³⁵⁰ As per the Privacy Engine Website definition Transfer impact assessment, also known as TIA, means that This is the process of evaluating the potential impact of transferring personally identifiable information from one context or location to another through a policy, program, or project, [https://www.privacyengine.io/data-privacy-management-software/records-of-processing-activities/transfer-impact-assessment#:~:text=What%20is%20a%20Transfer%20Impact%20Assessment%20\(TIA\)%3F,data%20Importer%20or%20data%20exporter](https://www.privacyengine.io/data-privacy-management-software/records-of-processing-activities/transfer-impact-assessment#:~:text=What%20is%20a%20Transfer%20Impact%20Assessment%20(TIA)%3F,data%20Importer%20or%20data%20exporter). (accessed on 1 July 2023).

¹³⁵¹ EDPS, EUDPR: Conditions and Safeguards in International Transfers to Private Entities, Transfer Impact Assessment Section, https://edps.europa.eu/system/files_de?file=2022-04/0167_2021-1047_01_redacted.pdf (accessed on 1 July 2023), p.94-95.

¹³⁵² EDPB (2023) Guidelines 01/2022 on data subject rights - Right of access Version 1.0, p.39.

¹³⁵³ EDPS comments on the Commission draft implementing decision amending Implementing Decision 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, p.2.

¹³⁵⁴ See Information from the processor to the joint controllers regarding the European Federation Gateway Service for the purpose of their Data Protection Impact Assessments (DPIA-Draft).

any sort of feared events associated with the interoperability processing activity. For instance, the DPIA set out in the relevant section that describes the requirements for a DPIA when the type of processing involves new technologies and may pose a high risk to individual rights and freedoms.¹³⁵⁵ Correspondingly, from our perspective, this guidance is the “golden source” of the interoperability activities, as it consist of massive amount of real-life related recommendations, as well as the elaborated technical and legal approach. Particularly, some of the risks pointed out by the DPIA recommendation are unlawful processing within the EFGS and processing interfering with the fairness requirement of Article 8 Charter¹³⁵⁶. Non-transparent processing, unauthorized disclosure or access to personal data, unauthorized transfer of personal data (to a third country), and so forth.

Therefore, it also alluded that our concerns related to the involvement of any third country is also valid as part of the feared events. To this end, in addition to what is brought by the DPIA recommendations, we believe that controllers should be able to implement their own TIAs and decide on whether they will involve in common structure for the interoperability matters. On controllers’ side, although Belgium, Croatian, Ireland, German¹³⁵⁷ applications and etc. publicly shared their DPIAs, they did not specifically deal with data transfers.

¹³⁵⁵ See Information from the processor to the joint controllers regarding the European Federation Gateway Service for the purpose of their Data Protection Impact Assessments (DPIA-Draft), p.18.

¹³⁵⁶ Article 8 of the Charter of Fundamental Rights of the European Union.

¹³⁵⁷For the full details of the referred DPIAs see, HSE DPIA <https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%202026.06.2020.pdf> (accessed on 23 June 2024); Corona Warn, DPIA https://www.fiff.de/dsfa-corona-file-en/at_download/FIfF-CoronaApp-DSFA-EN-v1.6.pdf (accessed on 23 June 2024); Stop COVID-19 app DPIA https://www.koronavirus.hr/uploads/Stop_COVID_19_Data_Protection_Impact_Assesment_Summary_2020_11_16_58dea76816.pdf (accessed on 23 June 2024); Corona Alert DPIA https://coronalert.be/wp-content/uploads/2021/07/DPIA_contactopsporingsapplicatie_BelgieV.8_NL_versie_17062021.pdf (accessed on 23 June 2024).

Within the same remit, the Commission's¹³⁵⁸ and the EDPB's¹³⁵⁹ existing work on the data transfer could also be leveraged to interoperability matters. Particularly, as detailed in previous sections is that use of contractual arrangements, such as standard contractual clauses for implementation of technical and organizational data protection law measures, ad hoc contractual clauses and international agreements/administrative arrangements, rather than implementing other referenced models such as binding corporate rules or certification, due to the mismatch between the nature of the applications and proposed model by the EU Commission and the EDPB. Thus, we are of the view that guidelines dealing with the interoperability matters could be more indicative in terms of the existing data transfer requirements applicable within the GDPR jurisdictions, by alluding the use of these, as data controller did not seem to rely on any data transfer regime in their documentation, rather than following the GDPR requirements.

On the of top of that, considering that the most important technical infrastructure provides of the many of the European applications, i.e., Google and Apple¹³⁶⁰ are the US based multinational corporations, and not limited to these companies, there is always risk exposure for interoperability matters both from data disclosure to the third countries perspective, and from the onwards transfers of the member state to third country perspective. Therefore, we believe that emphasize of the existing data transfer tools in the legal regime of the EU would be complementary to the interoperability framework created by the EU authorities and data controllers. Till date, though, we have not witnessed any feared data protection breach event associated with the

¹³⁵⁸ For further information see EU Commission Website, Rules on International Data Transfers https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en (accessed on 9 July 2023).

¹³⁵⁹ For further information see Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en (accessed on 9 July 2023).

¹³⁶⁰ See Apple Website, Newsroom, Apple and Google Partner on Covid-19 Contact Tracing Technology <https://www.apple.com/pl/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> (accessed on 10 July 2022).

use of GAEN architecture employed by the controllers reported to the authorities. Therefore, as a general assessment of each guidance/guideline analyzed here, we are of the view that the main actors of the EU for the data protection law activities provided a compatible holistic view in general, which allow data controllers to digest these requests within a short time. Accordingly, most of the data controllers also put their effort to act responsibly to facilitate interoperability feature of the applications, by actively taking part in Gateway joint controllers initiative, as also confirmed by the EU Commission. Majority of our assumptions for any potential use of these applications is based on the longer timeline of preparation, and actually it is the main target of our research to contribute to the data protection law literature. Nevertheless, it is important to remember that these high level or lack-of-detail perspective provided and critiqued in this Chapter, is at least positive in a regard that data controllers were provided with the freedom of the implementation of these core principles set out by the respective guideline/guidance. In general, as detailed, they mostly complied with the requirements, and till date, although there have been criticism and concerns on the certain aspect of various contact tracing applications, as detailed so far in this thesis, controllers seem to achieve compliance with multiple sources of information, i.e. various guidelines, in addition the existing data protection laws, based on their privacy documentation and non-existence of any drastic claim or penalty on this matter. Thus, while this is promising for the any potential use of these tools from European Data Protection Law perspective, there still are some points as delineated herein to maximize the implementation of core values of data protection law both from regulator and controllers' perspective in more concerted and streamlined manner by creating more holistic implementation. Particularly, to create less room for potential breaches, there seems to be a need for more detailed approach across the guidelines issued. Lastly, it is important to note that, there might be a need for further research in the future merely analyzing the commercial or political use of personal data by third parties, which were collected during the use of the applications. However, given the entirety of our research, this, by itself, do not fall within the scope our research.

**PART III- GENERAL LEGAL ASPECTS OF
PANDEMICS IN SPAIN, RADAR COVID
APPLICATION UNDER SPANISH DATA
PROTECTION LAW AND REGULATIONS:
FEATURES, RISKS AND RESOLUTIONS**

VI. SPANISH REGULATION OF PANDEMIC AND CONTACT TRACING APPLICATIONS

1. Constitutional Court Decision 148/2021 and Decreto de Alarma 463/2020

On the back of the analysis done for the EEA/EU applications, as delineated in the Introduction part, throughout this Chapter, our goal is to deep dive into the general legal framework of pandemic in Spain, before delving into digital contact tracing activities due to the characteristic of Spanish regulations enacted throughout the pandemic, which we believe can provide us with healthier opportunity to assess the data protection aspects of tracing activities in Spain in its entirety. Following to the analyses and recommendations on the general legal framework of pandemic, and healthcare implementation, we will accordingly deep dive into data protection matters during the pandemic term, and contact tracing framework through Chapter 6 and 7, by assessing data protection implementation and security risks of Radar Covid, and highly debated privacy concerns in light of the AEPD decisions and provide the main takeaways for both data controllers and regulators to achieve the most privacy friendly applications in Spanish jurisdiction. Therefore, this part of our research will specifically deal with jurisdictional nuances of Spain.

Accordingly, to establish the basis of the legal discussions, we would like to begin with the governmental decrees during the extraordinary case scenarios to handle respective situation, particularly Decreto de Alarma 463/2020, as it was opted by the government, and Constitutional Court decision thereon¹³⁶¹. Accordingly, to understand the implications and features of the Decreto de Alarma 463/2020, we believe that it is important to understand the legal structure that caused such legal safeguard, thereby entirety of the situation in Spain briefly.

¹³⁶¹ Decreto de Alarma 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 67, 14th March 2020).

Pursuant to article 116 of the Spanish Constitution¹³⁶² (“SC”), there are three different types of emergencies that can be declared: a state of alarm (“estados de alarma”) for natural disasters and other crises like epidemics; a state of exception (“estados de excepción”) for drastic and unusual changes in the public order; and a state of siege (“estados de sitio”) for assaults on Spanish sovereignty.¹³⁶³ Only the Spanish government has the authority to declare a state of alarm, which is the least restricted of the three situations of emergency.¹³⁶⁴ In situations of epidemics and medical emergencies, the

¹³⁶² Article 116 of the Spanish Constitution of 1978:

“1. Una ley orgánica regulará los estados de alarma, de excepción y de sitio, y las competencias y limitaciones correspondientes.

2. El estado de alarma será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros por un plazo máximo de quince días, dando cuenta al Congreso de los Diputados, reunido inmediatamente al efecto y sin cuya autorización no podrá ser prorrogado dicho plazo. El decreto determinará el ámbito territorial a que se extienden los efectos de la declaración.

3. El estado de excepción será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros, previa autorización del Congreso de los Diputados. La autorización y proclamación del estado de excepción deberá determinar expresamente los efectos del mismo, el ámbito territorial a que se extiende y su duración, que no podrá exceder de treinta días, prorrogables por otro plazo igual, con los mismos requisitos.

4. El estado de sitio será declarado por la mayoría absoluta del Congreso de los Diputados, a propuesta exclusiva del Gobierno. El Congreso determinará su ámbito territorial, duración y condiciones.

5. No podrá procederse a la disolución del Congreso mientras estén declarados algunos de los estados comprendidos en el presente artículo, quedando automáticamente convocadas las Cámaras si no estuvieren en período de sesiones. Su funcionamiento, así como el de los demás poderes constitucionales del Estado, no podrán interrumpirse durante la vigencia de estos estados.

Disuelto el Congreso o expirado su mandato, si se produjere alguna de las situaciones que dan lugar a cualquiera de dichos estados, las competencias del Congreso serán asumidas por su Diputación Permanente.

6. La declaración de los estados de alarma, de excepción y de sitio no modificarán el principio de responsabilidad del Gobierno y de sus agentes reconocidos en la Constitución y en las leyes”.

¹³⁶³ Utrilla, Dolores, García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) “Spain: Legal Response to Covid-19”, in Jeff King and Octávio LM Ferraz et al (eds), *The Oxford Compendium of National Legal Responses to Covid-19* (OUP 2021), pp.1-34, doi: 10.1093/law-occ19/e10.013.10.

¹³⁶⁴ Utrilla, Dolores, García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) “Spain: Legal Response...”, *op.cit.*, p.4.

Organic Law 4/1981¹³⁶⁵ (“L.O. 4/1981”) on the State of Alarm, Exception, and Siege permits exceptional measures restricting the full enjoyment of certain rights and freedoms.¹³⁶⁶ These measures include, among others, limiting the movement of people or vehicles at particular times and locations or necessitating that they meet specified requirements.¹³⁶⁷

Hence, Spain passed the first State of Alarm Decree on 14 March, i.e. Decreto de Alarma or also known as Royal Decree 463/2020, of 14 March.¹³⁶⁸ Correspondingly, Decreto 463/2020 (“the Decree”) authorized the Ministries of Health, Defense, Interior, Transportation, Mobility, and Urban Agenda to take all necessary steps to protect the health and safety of individuals, prevent the spread of the disease, and bolster the public health system, in addition to preventing and containing the virus and minimizing its negative effects on health, social, and economic systems, in accordance with the state of alarm provisions of L.O 4/1981. Following the blessing of the Spanish Congress of Deputies, the Government extended it a total of six times (RD 476/2020, of 27 March; RD 487/2020, of 10 April; RD 492/2020, of 24 April; RD 514/2020, of 8 May; RD 537/2020, of 22 May and RD 555/2020, of 5 June)¹³⁶⁹. The

¹³⁶⁵ Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio. «BOE» núm. 134, de 05/06/1981. <https://www.boe.es/buscar/act.php?id=BOE-A-1981-12774>.

¹³⁶⁶ The Law Library of Congress, Global Legal Research Directorate (2020) “Regulating Electronic Means to Fight the Spread of COVID-19” <https://tile.loc.gov/storage-services/service/ll/lglrd/2020714995/2020714995.pdf> (accessed on 23 June 2024), p.154.

¹³⁶⁷ *Ibid.*

¹³⁶⁸ Decreto de Alarma 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 67, 14th March 2020).

¹³⁶⁹ RD 476/2020, de 27 de marzo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 86, on 28th March 2020); RD 487/2020, de 10 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 101, on 11th April 2020); RD 492/2020, de 24 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la

previous three extensions have been part of the so-called de-escalation process, and each one has been ordered for a duration of fifteen days.¹³⁷⁰ The term of the prolongation stipulated in RD 555/2020, of June 5, 2020, concluded on June 21, 2020, marking the end of the State of Alarm in Spain.¹³⁷¹ The suitability of the declaration of this State of Alarm was, however, discussed by several scholars, and Constitutional Court also rendered a decision within the same direction, both of which will be detailed herein. Therefore, there were plenty of concerns raised against the severity of the decision, which is creating the center of attention for this section of Chapter 6 accordingly.

To begin with those debated aspects thereof, there is a source of concern regarding the extensive powers of authorities on the rights of individuals. To elaborate, allowing the competent authorities, in this case the Minister of Defense, the Minister of the Interior, the Minister of Transport, Mobility and the Urban Agenda and the Minister of Health, take not only those measures included in L.O. 4/1981 but any other measure necessary to fight the pandemic, although these must be included in regulations issued for this

situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 115, on 25th April 2020 ; RD 514/2020, de 8 de mayo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 129, on 9th May 2020; RD 537/2020, de 22 de mayo, or el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 145, on 23 May 2020 and RD 555/2020, de 5 de junio, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (published at BOE num. 159, on 6th June 2020).

¹³⁷⁰ García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain: an overview" Blog Droit Europeen available at :<https://blogdroiteuropeen.com/2020/06/29/covid-19-and-data-protection-in-spain-an-overview-by-rosario-garcia-mahamut/> (accessed on 23 June 2024).

¹³⁷¹ *Ibid.*

purpose.¹³⁷² Many scholars, which we also agree, support the idea that the limitations that could be established by the authorities provided in the Decree are way strong compared to the level of decision in this regard. To this end, more than fifty members of the Vox parliamentary group filed an appeal claiming that certain provisions of the Decree 463/2020, which was issued on March 14 and declared a state of emergency due to the Covid-19 pandemic, are unconstitutional.¹³⁷³ The appeal asserted violations of the following rights: the right to freedom of movement (Article 19 of the SC), the right to personal freedom (Article 17 of the SC), the right to assembly and free expression (Article 21 of the SC), and the principle of sanctioning legality (Article 25 of the SC), in addition to the violations of Article 55.1 (suspension of fundamental rights under the states of exception and siege) and Article 116 (emergency states) of the Spanish Constitution regarding the rights of assembly and demonstration (Article 21 of the SC) and the principle of sanctioning legality (Article 25 of the SC) regarding Article 7 of Royal Decree 463/2020 (lockdown); the right to education (Article 27 SC) regarding Article 9 (educative containment measures); the right to work (Article 35 of the SC); the freedom to conduct a business (Article 38 of the SC) regarding Article 10 (commercial activity containment measures) and the right to religious freedom (Article 16 of the SC) regarding Article 7 and 11 (religious containment measures).¹³⁷⁴

¹³⁷² García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain: an overview" Blog Droit Europeen available at :<https://blogdroiteuropeen.com/2020/06/29/covid-19-and-data-protection-in-spain-an-overview-by-rosario-garcia-mahamut/> (accessed on 23 June 2024).

¹³⁷³ Presno Linera, Miguel Ángel (2022) "The constitutional framework for collective health protection measures in the face of pandemics. SESPAS Report 2022", *Revista Direito Público*, n.94, Dossiê Especial-Covid-19, pp.15-34, p.15.

¹³⁷⁴ For the further details see Tribunal Constitucional de Espana, Sentencia 148/2021, de 14 de julio (Boe Núm. 182, de 31 de Julio De 2021), Ecli:Es:Tc:2021:148. In summary, the Constitutional Court invalidated certain parts of the Art.7 in Royal Decree 463/2020, which pertained to lockdown measures, citing that they violated the freedom of movement. Additionally, they found issue with the wording "modify, extend" in section 6 of Art.10 introduced by Royal Decree 465/2020. The Court upheld the constitutionality of the remaining measures. As for the implications, the Court mentioned that this

Nonetheless, it is important to note that the declaration of the state of alarm was not contested by the appellants; instead, Vox parliamentary group only argued that certain of the actions taken because of it were unlawful. Because of the appeal, as per the Constitutional Court, the declaration that the population's universal lockdown was unlawful has been the most important portion of the judgment. In this regard, as a quick recap, the Court has underlined that only the states of exception and siege permit the suspension of fundamental rights, whereas the state of alarm only permits the imposition of limitations.¹³⁷⁵

However, our assessment on the topic is that it is evidently difficult to establish the difference between restriction and suspension limits on the rights and freedoms of individuals living in the society, which we will address in the following pages. Therefore, interpreting the situation only based on the definitions would be vulnerable to further heated discussions. To this end, first of all, the Court has established a substantive definition of suspension in this regard. According to this description, a rule that prohibited all individuals from moving, anywhere or at any time, save in situations that were expressly deemed to be justifiable (lockdown), indicated the suspension of the right to freedom of movement, article 19 of the Spanish Constitution, which was prohibited during a state of alarm. For instance, as mentioned by Miguel Ángel Presno, regarding reasonableness of the limitations, their focus will center on how these measures affect specific vulnerable groups, as these measures constitute a limitation of movement that could significantly affect individuals within these communities, an acknowledgment also made promptly by the government,¹³⁷⁶ which we believe impact the type and content of the restrictions. The Court explained in the ruling that although the appellants

invalidation could prompt a review of criminal or administrative penalties imposed solely due to the nullified rules. Such a review might result in reduced penalties or absolution from responsibility. However, this declaration of unconstitutionality wouldn't enable claims holding the administration accountable.

¹³⁷⁵ Sentencia del Tribunal Constitucional 148/2021, de 14 de Julio (Boe Núm. 182, de 31 de julio de 2021).

¹³⁷⁶ Presno Linera, Miguel Ángel (2020) "Estado de alarma por coronavirus...." *op.cit.*, p.26.

have not raised those particular points, it should have been the state of exception that was proclaimed rather than the state of alarm as it ultimately was. The Covid-19 pandemic outbreak has been said to have put into doubt the public order, which is the state's enabling provision.¹³⁷⁷

Hence, from our perspective, the decision of the Court had triggered a few interesting discussions in the legal responses to Covid-19 literature. The first one is with regards to the choice of right legal basis for such suspension, whereas the second is related to terms of the difference between restriction and suspension. We all probably agree that the language of Constitution and L.O. 4/1981 on the State of Alarm is straightforward in a sense that does not leave lots of room for the selection of the right severity of the Decree, and it ties back to the above mentioned excessive powers granted to the relevant authorities. For a more tangible illustration, the declaration of a state of alarm is subject to subsequent parliamentary control, while the declaration of a state of exception necessitates prior authorization by the Parliament. Some scholars, such as Lorenzo Cotino, have argued that the quarantines imposed to deal with the Covid-19 crisis involve a suspension of that constitutional right and, therefore, the state of exception would be required, instead of state of alarm¹³⁷⁸. The reasoning of Cotino and other scholars who supported that it was suspension that rather than limiting freedom of movement, the Decree 463/2020 temporarily deprived entire populations from this right. For instance, regional elections in Euskadi and Galicia were called off, without an electoral legal provision to support, due to the state of alarm impacting the right to elect and be elected.¹³⁷⁹ Therefore, inevitably, during the pandemic

¹³⁷⁷ García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain: an overview" Blog Droit Europeen available at: <https://blogdroiteuropeen.com/2020/06/29/covid-19-and-data-protection-in-spain-an-overview-by-rosario-garcia-mahamut/> (accessed on 23 June 2024).

¹³⁷⁸ Cotino Hueso, Lorenzo (2021) "La (in)constitucionalidad de las restricciones y suspensión de la libertad de circulación por el confinamiento frente a la covid", Garrido López, C. (coord.) Excepcionalidad y Derecho: el estado de alarma en España, Colección Obras colectivas, Fundación Manuel Giménez Abad, Zaragoza. DOI: <https://doi.org/10.47919/FMGA.OC21.0004>, p.28.

¹³⁷⁹ Nogueira López, Alba, and Doménech Pascual, Gabriel (2020) "Fighting COVID 19 – Legal Powers and Risks". *Spain, VerfBlog*, 2020/3/30, <https://verfassungsblog.de/fighting-covid-19-legal-powers-and-risks-spain/>, DOI: [10.17176/20200331-013028-0](https://doi.org/10.17176/20200331-013028-0), p.1.

period in Spain, one of the hottest debate was regarding the notion of suspension of absolute fundamental rights, which we believe that one of the most fundamental discussion to address with regards to the essence of the Decree. Accordingly, we are also of the view that it is important to recall that neither the Spanish Constitution nor the L.O. 4/1981 of 1 June 1981 on states of alarm, exception and siege provided that any fundamental rights or public freedoms subject to constitutional complaint may be abrogated within the scope of the state of alarm.

On the other hand, as mentioned above, it is clear that the Spanish Constitution does not allow for the "suspension" of certain rights under a state of alarm; rather, it only permits these rights to be "suspended" in the case of a state of exception or siege¹³⁸⁰. Article 116.1 of Spanish Constitution permits the establishment of "limitations" during a state of alarm through L.O. 4/1981¹³⁸¹ permits the establishment of restrictions on goods that may be requisitioned, the freedom of movement at specific times or under specific conditions, the imposition of personal contributions, the intervention and temporary occupation of premises (apart from private homes), the limitation or rationing of the use or consumption of services or essential commodities, or the adoption of health and environmental protection safeguards.¹³⁸² Put differently, the declaration of a state of alarm does not take away a fundamental rights' essential nature or constitutional standing; rather, it permits the adoption of constraints or restrictions on the exercise of that right. Furthermore, it does not even momentarily halt the right's efficacy. The right must still be in effect and have access to all relevant constitutional guarantees, including effective judicial protection, respect for the fundamental elements of the right as stated in Article 53.1 of the Spanish Constitution, weighing

¹³⁸⁰ See Article 55.1 of the Spanish Constitution.

¹³⁸¹ See Article 11 of L.O. 4/1981.

¹³⁸² See the Report of Venice Commission (European Commission For Democracy Through Law), Venice Commission - Observatory on emergency situations <https://www.venice.coe.int/files/EmergencyPowersObservatory/ESP-E.htm> (accessed on 26 September 2023).

proportionality when enforcing restrictions, and protection through filing a constitutional complaint with the Constitutional Court.¹³⁸³

Nonetheless, in this point, the second dimension of the issue has come into the play, which we find extremely significant to address the essence of such suspension of rights rather than simply rejecting the necessity of such implementation resulted from the Decree. To provide more specific detail with the discussion point, while suspension is allowed out under the Spanish Constitution only for state of exception and siege, as per Article 55.1.¹³⁸⁴ it is still, as per Article 116.1¹³⁸⁵, as also supported by Escobar, who provided that the measures were unconstitutional because they were regulated as if in a state of exception,¹³⁸⁶ possible to apply certain restrictions during state of alarm, as detailed above. Similarly, within the same context, Amoedo-Souto provided that irrespective of its health purpose, the nature of this forced confinement is not merely a limitation or compression of the exercise of these fundamental rights in certain places, moments, or public spaces but a general suspension of them, and it, would have required, as a prerequisite, a declaration of a state of exception.¹³⁸⁷ On the other hand, de Gatta and Dionisio Fernández claimed that, the Royal Decree declaring the state of alarm, or subsequent decrees, may decide on the following measures: limit the movement or presence of people or vehicles at specific times and places, or subject them to certain requirements (but not the suspension of the free movement of persons, as per article 19-CE); temporarily requisition any type of goods and impose mandatory personal services; intervene and temporarily

¹³⁸³ *Ibid.*

¹³⁸⁴ For the full article see article 116.1 of the Spanish Constitution Passed by the Cortes Generales in Plenary Meetings of the Congress of Deputies and the Senate held on October 31, 1978 Ratified by the Spanish people in the referendum of December 6, 1978 Sanctioned by His Majesty the King before the Cortes on December 27, 1978.

¹³⁸⁵ *Ibid.*

¹³⁸⁶ Guillermo Escobar, Roca (2021) "Los derechos humanos en estados excepcionales y el concepto de suspensión de derechos fundamentales." *Revista de Derecho Político*, vol.110, pp. 113-152.

¹³⁸⁷ Amoedo-Souto, Carlos Alberto (2020) "Vigilar y castigar el confinamiento forzoso: problemas de la potestad sancionadora al servicio del estado de alarma sanitaria", *El Cronista del Estado Social y Democrático de Derecho*, n. 86-87, pp. 66-77.

occupy industries, factories, workshops, operations, or premises of any nature.¹³⁸⁸ Therefore, as seen there are different understandings and interpretation on this decree when it comes to its essence. Thus, we believe that these views are highly debatable, as there is not any concrete and direct response to the most important issues; namely what are the scope of suspension of these fundamental rights that was provided by the Decree? The same question was also asked by Lorenzo Cotino Hueso, as he called out that an important and complex debate is whether the State of Alarm Decree suspended rights, particularly the freedom of movement, should be clarified.¹³⁸⁹ The underlying reason of this question is, while for some, the first state of alarm declared in Spain allowed for the limitation (not suspension) of certain fundamental rights: freedom of movement, temporary requisition of goods and properties as industries, workshops or venues with the exception of private residences, limit or ration first need goods or services, or make all necessary arrangements to guarantee market supply (during the state of alarm).¹³⁹⁰ The similar debate was also reiterated by different scholars before the Constitutional Court decision, such as Durán Alba, who also mentioned the "sense" that freedom of movement has been suspended, asking, "What greater restriction in terms of freedom of movement could there be, to accurately refer to a scenario of suspension?"¹³⁹¹ Identical stance was also taken by Álvarez García who echoes this sentiment, questioning what would

¹³⁸⁸ de Gatta Sánchez, Dionisio Fernández (2020) "Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el covid-19 y sus prórrogas." *AIS: Ars Iuris Salmanticensis*, vol. 8, no. 2, pp. 192-199, p.198.

¹³⁸⁹ Cotino Hueso, Lorenzo (2021) "La (in)constitucionalidad de las restricciones y suspensión de la libertad de circulación por el confinamiento frente a la covid", Garrido López, C. (coord.) *Excepcionalidad y Derecho: el estado de alarma en España*, Colección Obras colectivas, Fundación Manuel Giménez Abad, Zaragoza. DOI: <https://doi.org/10.47919/FMGA.OC21.0004>, p.28.

¹³⁹⁰ Civil Liberties Organisations Across the European Union (2020) "EU 2020: Demanding On Democracy Country & Trend Reports on Democratic Records, Spain" https://dq4n3btxmr8c9.cloudfront.net/files/6th9cw/Liberties_RoL_report_2021_SE.pdf p.25. (accessed on 30 September 2023).

¹³⁹¹ Durán Alba, Juan Fernando (2021) "Afectaciones a la libertad de circulación derivadas del estado de alarma declarado a causa de la crisis «Covid-19»", en Biglino Campos, Paloma y Dyrán Alba, Juan Fernando (dirs.) *Los efectos horizontales de la Covid-19 sobre el sistema constitucional: estudios sobre la primera oleada*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, pp. 193-220, p.215.

be needed to consider it a suspension of freedom of movement, calling it "absurd" not to consider it suspended "when the only thing allowed is movement from one's kitchen to the bedroom."¹³⁹² Likewise, Sánchez Ferriz also affirmed the existence of suspension in this particular matter.¹³⁹³ Therefore, as seen, there were plenty of legal discussions around the notion of suspension of rights, and whether such suspension actually took place or not during the validity of the Decree, and whether the selection of the Decree was the legally most accurate one. Accordingly, as much as we find all of these discussions very much helpful to understand the nature of the notion, Decree and situation in Spain, we would like to reflect on the judgements of the Constitutional Court, which rendered its decision on this very matter.

Correspondingly, in its detailed judgment, the Constitutional Court has attempted to differentiate between the terms "limitation" and "suspension," stating that the former is the most general phrase and the latter the most precise, and that a suspension consequently comprises a qualified limitation. It was tantamount to a temporary halt of the enjoyment of fundamental rights and their protections. In other words, as per the Constitutional Court, a "suspension" signifies a halt, albeit temporary, in the exercise of fundamental rights and their protections. As such, the Court favored a substantive interpretation of suspension over a formal one, determining it as a profound restriction of a fundamental right rather than a provisional annulment of the constitutional provision acknowledging that right.¹³⁹⁴ Accordingly, by establishing the existence of suspension of rights during the pandemic, as detailed above, the Court partially nullified certain provisions that restricted freedom of movement and empowered the Minister of Health to modify containment measures in economic establishments and activities, and these restrictions were deemed excessive and not adequately bounded within the

¹³⁹² Álvarez García, Vicente (2020) "El coronavirus (COVID-19): respuestas jurídicas frente a una situación de emergencia sanitaria", *El Cronista del Estado Social y Democrático de Derecho*, monográfico Coronavirus... y otros problemas, marzo-abril 2020, pp. 6-21, p. 12-13.

¹³⁹³ Sánchez Ferriz, Remedio (2020) "Reflexiones constitucionales desde el confinamiento", *en Actualidad Jurídica Iberoamericana*, núm. 12 bis, pp. 16-23, p. 21.

¹³⁹⁴ Nogueira López, Alba; Doménech Pascual, Gabriel (2020) "Fighting COVID 19...", *op.cit.*, p.1.

framework of constitutional rights and principles.¹³⁹⁵ Nonetheless, our assessment on the topic is that while we also agree that freedom of movement is more severe than a limitation, therefore, it should not have been provided under state of alarm decree, at the same time, due to the controversial nature of suspension and limitation, some might also come up with perspective that such measures were not entirely deemed as suspension. Therefore, it requires further justification of what is deemed as limitation and suspension, and thereby exceeding the limits of Decreto de Alarma.

Accordingly, in this very point of the heated discussions, we believe that the most optimal and balanced response were provided by the dissenting opinion¹³⁹⁶ of Judge Maria Luisa Balaguer Callejón on this matter, as they provided a focus on other aspects of the heated discussions. In more detail, Maria Luisa Balaguer Callejón announced the publication of the judgment in the Official State Gazette and included a separate dissenting opinion from the President of the Court, highlighting discrepancies in the legal reasoning and the judgment. As a high-level summary of her dissenting opinion, they provided that the resolution of the aforementioned controversy must first consider whether such exceptional constraint imposed by sections 1 and 3 of Article 7 of Royal Decree 463/2020 conforms to what is provided for in the Organic Law 4/1981 referred to by Article 116.1 of the Constitution. If this is indeed the case, it would be necessary to analyze whether its scope could be qualified as a "suspension" of the right, prohibited for the state of alarm, and whether the limitation respects the requirements of proportionality. We believe, thus, this dissenting opinion is playing the key role to complement and conclude the aforementioned discussions of scholars presented and broken down into pieces namely existence of suspension and respecting to the proportionality, which we address in the last part of this sub-chapter.

¹³⁹⁵ Sentencia del Tribunal Constitucional 148/2021, de 14 de Julio.

¹³⁹⁶ For the full dissenting opinion of Judge Maria Luisa Balaguer Calalejon, member of Constitutional Court, see "Fundamento Jurídico 5" of Sentencia del Tribunal Constitucional 148/2021, de 14 de Julio (Boe Núm. 182, de 31 de julio de 2021), pp. 28-33.

As per the details of the dissenting opinion, Judge Balaguer Callejón first provided that under the heading "limitation of the freedom of movement of persons," Article 7, in its sections 1 and 3, did not merely define the scope of that freedom, as is the case with other rules established for situations of normalcy. Instead, it drastically limits or restricts it to the extent of altering or temporarily excepting its essential content.¹³⁹⁷ In other words, they clearly indicated, which is also in our approach that will be detailed in the following pages, that it is not really possible to clearly define the scope of the notion of suspension and, even if it were, I believe that the ruling does not achieve it either. So the classification of home confinement as a suspensive measure of freedom of movement ends up seeming like an exercise in voluntarism loaded with subjectivity, among other reasons because it forgets that the restriction of movement was not absolute, to the extent that a high level of movement was contemplated.¹³⁹⁸ Also, number of exceptions and reasons that justified leaving home. Accordingly, as we discussed above, it makes sticking with one-fits-for-all type of definition of suspension, and therefore its potential legal boundaries.

As such, with regards to the selection of the type of emergency, they opined that the nature of the risk to the constitutional system is different in the state of alarm and in the state of exception. In either case, the declaration of the exceptional state implies the possibility of adopting measures aimed at controlling or reversing the emergency situation that justifies that adoption.¹³⁹⁹ For this reason, Organic Law 4/1981 associated with the state of alarm measures linked to the management of the material crisis, without ruling out those that may limit the exercise of rights, while the state of exception is associated with the adoption of clearly defined restrictive measures (suspensive according to art. 55 CE) of those fundamental rights that, if exercised in an ordinary way in the context of the identified constitutional

¹³⁹⁷ Dissenting opinion of Judge Maria Luisa Balaguer Calalejon, *op.cit.*, p.29.

¹³⁹⁸ Dissenting opinion of Judge Maria Luisa Balaguer Callejón, *op.cit.*, p.29.

¹³⁹⁹ Dissenting opinion of Judge Maria Luisa Balaguer Callejón, *op.cit.*, p.29.

crisis, could reinforce that same situation as well as the situation of alteration of public order that has led to the declaration of the state of emergency. Thus, they provided that considering this aspect, the appropriateness was actually present in the Decree, because there was a constitutionally legitimate purpose for adopting restrictive measures, namely the preservation of public health. In more detail, the confinement was directly intended to control the progression of the disease causing the health crisis, that is, to preventively protect the health of citizens (art. 43 CE), this guiding principle being closely connected to the preservation of the right to life and physical integrity (art. 15 CE). Suitably, we are also of view that the appropriateness, necessity and urgency were existing the situation in Spain, and in many other countries as well, considering that this pandemic negatively impacted many other aspects of individuals' lives, alongside with right to life and physical integrity.

From our perspective, they also further justified this approach, by pointing out the other most significant component of the legitimate safeguards, namely proportionality and legitimacy, which we will elaborate in the following pages. To this end, they provided that the measures adopted could also overcome a proportionality judgment in the strict sense.¹⁴⁰⁰ The restriction of freedom of movement contained in art. 7 of the Decree, despite being severe, was not disproportionate, taking into account the need to guarantee the right to health of citizens in the context of shortages of medical equipment, materials and humans, existing at the time they were adopted. Furthermore, such questioned measures, and the equivalent situation that was being experienced in almost all countries, which we also agree with this fact. Thus, the undeniable sacrifice inflicted on the fundamental right to freedom of movement cannot be understood as superior to the benefit obtained, at that time, in relation to limiting the exponential contagion of the virus, which would have had an irrecoverable impact on the right to life of many people, and intensely on the right to health of an even greater number.¹⁴⁰¹ Hence, they

¹⁴⁰⁰ Dissenting opinion of Judge Maria Luisa Balaguer Calleón, *op.cit.*, p.30.

¹⁴⁰¹ Dissenting opinion of Judge Maria Luisa Balaguer Callejón, *op.cit.*, p.31.

were of view that the safeguards as part of the Decree were proportionate for this reason.

Accordingly, in the end of her dissenting opinion, they concluded that considering that it was not possible to simultaneously declare both the state of alarm and the state of exception, thus, either everything becomes unconstitutional due to the inadequacy of the identified exceptional state, or nothing does, as it is impossible to separate the measures adopted across various regulatory instruments.¹⁴⁰² That being said, we would like to highlight the reason of such discrepancy they pointed out, which we believe creates the main heated discussions around the type of state of emergency selected. As per her opinion, there are difficulties that have arisen from the contrast between the Constitution, the Organic Law 4/1981, of the states of alarm, exception and siege, and the Decree 463/2020, of March 14 (arts. 7, 9, 10 and 11), by which the state of alarm was declared for the management of the health crisis caused by COVID-19 (and subsequent ones) subject to control of constitutionality, which we agree again. However, despite such differences, they concluded that it must be concluded that Organic Law 4/1981 perfects the regulation of the constitutional right of exception, thus becoming an integral part of the block of constitutionality, understood as a control parameter of norms with the rank of law such as the decree declaring the state of alarm.¹⁴⁰³

Correspondingly, in light of aforementioned facts, we do have couple of thoughts and takeaways from her dissenting opinion to better address the aforementioned discussions exacerbated by the Constitutional Court decision, and scholars varying opinions. First of all, our assessment and

¹⁴⁰² Álvarez Vélez, M. Isabelle (2021). "Alarm and pandemic: legal-constitutional problems of states of necessity in light of the doctrine of the Constitutional Court: Comments on the Constitutional Court Ruling 148/2021, of July 14, unconstitutionality appeal no. 2054-2020. (BOE no. 182, of July 31, 2021); to the Ruling of the Constitutional Court 183/2021, of October 27, unconstitutionality appeal no. 5342-2020. (BOE no. 282, of November 25, 2021); and to the Ruling of the Constitutional Court 168/2021, of October 9. Appeal for protection no. 2109-2020. (BOE no. 268, of November 9, 2021)". *Magazine of the Cortes Generales*, (111), pp. 547-574.

¹⁴⁰³ Dissenting opinion of Judge Maria Luisa Balaguer Callejón, *op.cit.*, p.31.

recommendation on the entirety of the issue is that, by their essence, instead of merely agreeing with the definitions rendered by the Constitutional Court on the distinction between the suspension and restriction, we would like to offer more adjusted approach for individuals in terms of interpretation of these fundamental rights and their potential restrictions by prioritizing the safeguards that needs to be put in place by the Government, which is more aligned to what judge Balaguer Callejón provided, as detailed above. We, accordingly, would like to emphasize the importance of the existence of legal, safeguards and proportionality, including oversight mechanism during the validity of the restriction, rather than the type of the selected restriction. On the top of that, usage of extremely detailed legal justification on any selected suspension or restriction, which triggers such necessities, and is selected as only the last resort in the circumstances. Nevertheless, we must also agree the fact that in legal practice, these terms and justifications are always open to different interpretation of different scholars, legal practitioners and judges. Therefore, even though we would like to emphasize the significance of safeguards and justifications to be implemented to protect individuals, rather than terminological discussions, some scholars or legislators might not agree with our approach as they may believe in the certainness of certain legal concepts, and their strict implementation, to provide arbitrariness in the interpretation. Suitably, in this point, we must also admit that the use of restrictions in its general sense, rather than suspensions of rights in the form of what the Court defined as extreme and what is happening in vast majority of cases, which we believe is more in line with our era, and in with the approach brought by significant Covenant and Conventions in force. To provide more specific sample, as per International Covenant on Civil and Political Rights, every individual who is in a State's territory legally has the entitlement to move freely and decide where they want to live within that territory. These rights mentioned above should not face limitations, except when such restrictions are defined by the law, serve the purpose of safeguarding national security, maintaining public order, preserving public the protection of morals or health, or the safeguarding the rights and freedoms of others and aligning with the other rights acknowledged in the present

Covenant.¹⁴⁰⁴ Likewise, pursuant to European Convention on Human Rights, no restrictions shall be imposed on the exercise of these rights except those prescribed by law and deemed essential in a democratic society for reasons of national security or public safety, the preservation of public order, crime prevention, safeguarding morals or health, or preserving the rights and freedoms of others..¹⁴⁰⁵ Even though on the ideal level it is beneficial for our approach to observe that these fundamental covenant and conventions recognize the restriction with public health and other individuals' rights and freedoms necessities, as seen, they provided very limited and defined open door for certain restrictions refer to restrictions in the existence of these legal justifications. Accordingly, we must also understand the essence of what Judge Balaguer Callejón provided for the trade-off created by the circumstances. We concur with the idea that the undeniable sacrifice inflicted on the fundamental right to freedom of movement cannot be understood as superior to the benefit obtained. As such, although technically the term of suspension is made possible by law under state of exception and siege, as debated by the scholars, we believe that implementing limited and proportionate restrictions on these fundamental rights with the well-defined legal boundaries and timeline is more compatible with the general spirit of rights and laws, rather than creating extensive derogations. In addition to this dissenting opinion, we must also add that, still, on the positive side, it is plausible to observe that in Spanish system, there has been no decision to derogate from the ECHR ¹⁴⁰⁶ or any other international human rights convention,¹⁴⁰⁷ which at least indicated that existence of aforementioned intrusiveness of the rights during the emergency state, still till date, the

¹⁴⁰⁴ See Article 12 of International Covenant on Civil and Political Rights <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (accessed on 28 October 2023).

¹⁴⁰⁵ See Article 2.3 of the European Convention on Human Rights.

¹⁴⁰⁶ For the entirety of the Convention see European Convention On Human Rights <https://www.echr.coe.int/european-convention-on-human-rights>.

¹⁴⁰⁷Utrilla, Dolores; García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) "Spain: Legal Response... ", *op.cit.*, p.4.

intention of the limitation put in place in Spain was not to derogation from the main fundamental human rights.

On the other hand, we believe it is a decision very much in line with our approach, the Supreme Court of Spain (“*Tribunal Supremo*”) did not seem to be impacted by this terminological discussions. To pinpoint their explanation to fortify our approach, in its decision on Cassation Appeal Number 3375/2021¹⁴⁰⁸, the Supreme Court emphasized that adoption of restrictive measures (such as tailored restrictions on freedom of movement, which is the only type of measure specifically addressed in this ruling) is subject to four cumulative requirements, namely that: (i) there is a serious transmissible disease that endangers the health and life of individuals; (ii) the restrictive measure is essential to prevent transmission because there are no other effective measures; and (iii) the restrictive measure is essential to prevent transmission, (iv) the limiting measure has a precise time frame that is established in light of what is required to stop the illness from spreading.¹⁴⁰⁹

Hence, as seen, it is vital to understand the essential components of such restrictions in terms of their contents as Tribunal Supremo did, in order to agree the existence of such legal justification, and not to abuse any freedom of individuals, rather than merely struggling with the terminological nuances and could implement the required safeguards with more clarity on whether it is last resort, urgently needed and proportional. The main reason is that there is sometimes not any black and white approach on this type of important terminological distinctions in the legal literature, because if we take a technical perspective, in principle, we agree with the decision rendered by the Constitutional Court that such suspensions were unlawful, and Decreto de Alarma was not the right lawful basis selected for this pandemic within the

¹⁴⁰⁸ For the full decision see Tribunal Supremo. Sala de lo ATS 3375/2021 - ECLI:ES:TS:2021:3375A Contencioso <https://www.poderjudicial.es/search/documento/AN/9470383/actos%20y%20procedimiento%20administrativo/20210330> (accessed on 23 June 2023).

¹⁴⁰⁹ Utrilla, Dolores (2020) “Spanish Supreme Court clarifies legal framework of restrictive measures adopted under public health legislation”, Lex-Atlas: Covid-19 available at: <https://lexatlas-c19.org/spanish-supreme-court-clarifies-legal-framework-of-restrictive-measures-adopted-under-public-health-legislation/> (accessed on 23 June 2024).

Constitution. Nonetheless, from our perspective, Judge María Luisa Balaguer Callejón's dissenting opinion is far more convincing due to the aforementioned reasons.

Above all, our assessment on the topic is that selection of accurate technical wording is not the only problematic aspect and that aforementioned elements of any restriction are the most vital necessity of any pandemic related decree/ We are of view that, which was also pointed by judge Balaguer Callejón's opinion, proportionality, legitimacy and necessity of the limitations at stake must be clearly indicated and justified by the legislators in any type of pandemic scenarios. In other words, from our angle, as also detailed by Venice Commission that regardless of the level of relevant degree, it is quite important to implement these measures in line with the necessity and proportionality requirements ¹⁴¹⁰, which are of vast significance to the efficiently working law and regulations and providing extremely clear and narrowly interpreted justifications. Thus, to put it differently, pandemic decrees and other relevant orders should be less restrictive and more proportional in the first place, rather than suspension of rights of individuals, yet in any case, on the top this distinction, both suspension and restriction of rights should ideally be based on a legal framework, subject to relevant checks by the courts, and proportional to the situation at hand, which we believe are creating most remarkable components of such limitations, rather than one-fit-for-all type of approach set out in the existing regulations. More importantly, governments must justify these actions as necessary and not arbitrary to be more resilient against this pandemic type of emergency situations from legal perspective as well. In case there is any restriction on rights, it must be compatible with legality, necessity, proportionality, non-discrimination, and

¹⁴¹⁰ See the Report of Venice Commission (European Commission For Democracy Through Law), Venice Commission - Observatory on emergency situations <https://www.venice.coe.int/files/EmergencyPowersObservatory/ESP-E.htm> (accessed on 26 September 2023).

strict interpretation.¹⁴¹¹ Therefore, we are of the view that what Alessandra Pierucci, Consultative Committee of Convention 108, provided should establish the ground floor for all of the restrictions.¹⁴¹² To this end, justification and clear explanation of any restrictive action should be provided for closing any legal misinterpretation of the issue, in line with our general transparency approach provided in previous Chapters, probably for the wider sense, not limited with data protection law, which would also positively impact on the perception of individuals in society to reduce their fears about any excessive limitation of their fundamental rights imposed by authorities to tackle the pandemic. To put differently, more clarity on the intended distinction of suspension of rights and its reasons, justification, proportion, duration, and potential consequences must be clearly indicated, so that such ambiguities should not arise going forward.

2. Need for a new health regulation of pandemics

On the top of aforementioned discussions resulted from the ambiguity of the pandemic atmosphere, it is also important to delineate that such ambiguity can and should be mitigated by the existence of a more specific regulation dealing with the pandemic measures and any potential limitation as a consequence of such measures. As seen, there have already been plenty of debates around the type of legal basis and the level of the Decree, as detailed in the previous section, which can be easily found through many sources. As such, we believe that it increased the importance of other healthcare regulations in force to effectively manage the situation, rather than putting a decree on the center of pandemic management in Spain. Nevertheless, we

¹⁴¹¹ United Nations (2020) “Emergency Measures and Covid-19”, https://www.ohchr.org/sites/default/files/Documents/Events/EmergencyMeasures_COVID19.pdf (accessed on 23 June 2024), p.2.

¹⁴¹² Alessandra Pierucci provided on Covid-19 and Data Protection relation is that in light of the unprecedented situation we are dealing with, it is imperative to avoid the urge to indiscriminately suspend the protection of basic rights without conducting a comprehensive analysis of the proportionality and effectiveness of the proposed actions. In order to safeguard the population without placing society at greater risk in the long run, it is essential to ensure the rule of law, respect for human rights, and democracy. Available at: <https://www.coe.int/en/web/data-protection/covid-19-data-protection>.

also believe that it is important to analyze the situation in Spain precisely, as each county has their own characteristics. As known, Spain is a semi-federal or regional state, also known as a State of Autonomies, and has seventeen Autonomous Communities (ACP) and two Autonomous Cities (Ceuta, Melilla).¹⁴¹³ Each Autonomous Community possesses its own legislature, executive, and electoral frameworks mirroring those established at the national level, maintain the management of public health services.¹⁴¹⁴ Therefore, in other words, as a natural consequence of this legal framework, under the decentralized Spanish system (*Estado autonómico*), the seventeen regional Autonomous Communities have health competences transferred to them, with the state at the national level being responsible for certain strategic areas, as well as for the overall coordination of the National Health System.¹⁴¹⁵ More specifically, the Spanish Ministry of Health has responsibility for national plans, regulation and laws, and the Departments of Health of the Autonomous Communities are responsible for the regional implementation of national regulations and for the development of regional regulation and policies.¹⁴¹⁶ Local authorities have relatively residual competences for the protection of public health in terms set out in national and regional legislation (Article 25(2) of Law 7/1985 of 2 April establishing the Bases of the Local Regime¹⁴¹⁷). All these levels of administration have employed a mix of binding and non-binding preventive measures to contain the spread of the virus. Accordingly, there were a few orders passed to complement these binding and non-binding measures, such as contact tracing procedures that were established by nonbinding protocols approved by the Minister of Health and updated on a

¹⁴¹³ Fernandez-Bermejo Utrilla, Dolores (2021) "Soft Law Governance in Times of Coronavirus in Spain", *Eur J Risk Regul.*, vol.12, n.1, pp.111-126.

¹⁴¹⁴ Martín Guardado, Sergio (2020) "Real Decreto 463/2020, de 14 de marzo, sobre el estado de alarma", *AIS: Ars Iuris Salmanticensis*, vol. 8, no. 2, pp. 223-228, p.228.

¹⁴¹⁵ Fernandez-Bermejo Utrilla, Dolores (2021) "Soft Law Governance...", op.cit., p.112.

¹⁴¹⁶ *Ibid.*

¹⁴¹⁷ Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. <https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392>.

constant basis on from 14 March 2020 onwards,¹⁴¹⁸ or likewise, the Minister of Health issued an order mandating all public and private health centers, as well as health workers, to report all confirmed and suspected cases of Covid-19 to the Ministry of Health. Additionally, the surveillance protocols ratified in the National Health System's Interterritorial Council were enforced nationwide,¹⁴¹⁹ and the surveillance protocols agreed in the National Health System's Interterritorial Council were made mandatory all over the country.¹⁴²⁰ Hence, in short, as seen, there are plenty of orders, decrees, guidelines were provided to manage the different bits of surveillance and contact tracing activities from different perspective and scope to complement the actions detailed in the previous sections of this Chapter.

Nevertheless, in light of this summarized structure of Spanish legal aspects of healthcare system, it is important to highlight the fact that the main actors, around which the pandemic issues revolved are the following three main central laws, which contains several provisions that satisfy these constitutional requirements and allow the abovementioned measures to be taken without much difficulty, including those that interfere with the exercise of fundamental rights. These measures were adopted by regional governments pursuant to L.O. 3/1986, of 14 April. This legislative act grants health authorities a very wide discretion in this regard, as it empowers them to adopt any measure they deem necessary in the case of a transmission risk¹⁴²¹. Other central state level laws such as Act 14/1986, of 25 April on general health, Act 17/ 2015, of July 9 on the national civil protection system and Act 33/2011, of 4 October on public health empower health authorities to

¹⁴¹⁸ Ministerio de Sanidad (2020), 'Procedimiento De Actuación Frente A Casos De Infección Por El Nuevo Coronavirus (Sars-Cov-2)' (14 March 2020) http://www.aeemt.com/web/wp-content/uploads/2020/03/2020-03-14_-_Procedimiento-COVID_19.docx.pdf (accessed on 23 June 2024).

¹⁴¹⁹ Order SND/404/2020 (Minister of Health) (11 May 2020). <https://www.boe.es/buscar/act.php?id=BOE-A-2020-4933>.

¹⁴²⁰ See Article 24 of Royal Decree-law 21/2020 (9 June 2020), <https://www.boe.es/buscar/act.php?id=BOE-A-2020-5895>.

¹⁴²¹ See Article 3 of Ley 14/1986, de 25 de abril, General de Sanidad.

impose personal obligations on retired or trainee health workers, requisitions of goods, obligations on the population to cooperate with the police etc. In other words, during the Covid-19 crisis these three pieces of existing state-level legislation have been relied on as the main tools to adopt emergency public health measures.¹⁴²²

Correspondingly, to begin with the first main law, namely L.O. 3/1986, of 14 April, after briefly delineated the general structure of the Spanish legal system on healthcare matters, we can initially provide that there is a complex structure and each of the measures implemented are based on pursuant to L.O. 3/1986. Therefore, we automatically, in line with spirit of this research, are tempted to investigate whether such old legislation is still fit-for-purpose given the complexity of legal structure and growing new challenges resulted from new types of pandemics. The law itself set out that the competent health authorities may adopt recognition, treatment, hospitalization or control measures when rational indications are observed that allow us to assume the presence of hazard to the health of the individuals due to the specific health situation of a person or group of people or due to the conditions health conditions in which an activity is carried out.¹⁴²³ Thus, as seen, it gives an extensive and open-ended powers to relevant competent health authorities in Spain, as there is not any specific situation delineated, rather than general situations of detriment to public health. Moreover, according to the Law, for the purpose of managing communicable diseases, the health authority has the authority not only to implement general preventive measures but also to undertake suitable actions to manage the individuals who are ill, those who have been in contact with them, and the surrounding environment.¹⁴²⁴ On the top of that, as another vast authority attributed to the authorities, the Law stated that when a medicine, a health product or any product necessary for the protection of

¹⁴²² Utrilla, Dolores; García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) "Spain: Legal Response...", op.cit. p.5.

¹⁴²³ Article 2 of Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

¹⁴²⁴ Article 3 of Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

health is affected by exceptional supply difficulties and to guarantee its better distribution, the State Health Administration may, temporarily establish centralized supply by the Administration, and can make its prescription conditional on the identification of risk groups, performance of analytical and diagnostic tests, completion of protocols, sending to the health authority of information on the course of treatments or other similar particularities.¹⁴²⁵

Consequently, as seen, wide range of high-level situations are described in the Law. On the other hand, although we find it positive to observe such approach that prioritize public health no matter what, there would be more solid and elaborated approach is need for other fundamental rights that are impacted by the existence of such pandemic situation alongside with these rights. For example, as put forward by Amoedo-Souto recently, the people of Spain diligently and sacrificially complied with the public obligation to confine themselves in their homes.¹⁴²⁶ Intense fear and uncertainty prevail, not only about the disease but also about the looming economic situation. Even under the threat of the coronavirus, we should not relinquish our citizen rights with guarantees, without compromising the effective fight against the pandemic.¹⁴²⁷ Therefore, we understand that despite the presence of necessities of compromising, it may not be possible to cover everything in a single short text published by central government, yet, there might still be chance to set out further nuances of these with more elaborated legislation, due to which we believe that there is a need for a proper and detailed approach for pandemic related safeguards in society that may also impact fundamental rights of individuals, accountabilities of institutions, rights of individuals against these safeguards. To this end, similarly, Nogueira López and Doménech Pascual also put forward the idea that, this situation demonstrates how the emergency laws enacted in 1981 are ill-suited to handle health emergencies, particularly significant ones like the COVID-19

¹⁴²⁵ See Article 4 of Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

¹⁴²⁶ Amoedo-Souto, Carlos Alberto (2020) "Vigilar y castigar el confinamiento forzoso...." op.cit., p.77.

¹⁴²⁷ Amoedo-Souto, Carlos Alberto (2020) "Vigilar y castigar el confinamiento forzoso...." op.cit., p.77.

pandemic. The breadth and bounds of legislative control and judicial review are not precisely determined by its provisions. They failed to consider that Spain is a decentralized state, with regions having competence over health-related issues. Due to the Minister of Health's inexperience in day-to-day health care administration, the concentration of emergency powers might have unfavorable effects. Furthermore, the imposition of increasingly stringent quarantines, which momentarily deny the freedom of movement to whole communities, poses major issues with the notion of democracy.¹⁴²⁸ Accordingly, we agree with the perspective brought by them for the lack of clarity on the scope and boundaries of parliamentary control for pandemic scenarios. Such ambiguity would potentially cause a risk of arbitrariness, which would contradict with the principle of democracy, as central government is equipped to take any sort of action with regards to the implementation of healthcare rules without any definitive boundaries. Also, as Nogueira López and Doménech Pascual rightly mentioned that we agree with their thoughts on centralization of emergency power might end up in a situation where inefficient outcomes could be generated for day to day management of the pandemic issues in each and every state, given that current Spanish health law already gives wide array of extraordinary powers to the relevant authorities.¹⁴²⁹

Thus, it would probably make more sense to defer some of the day-to-day related tasks to the local governments, as they have more close affinity with the issues and needs in their region. However, different than their views, we are of the view that centralization of pandemic management, on the other hand, would result in less time-consuming decision making, quicker action to be generated, and creating the parameters of targeted situation,¹⁴³⁰ which would create an advantage given the quickly evolving nature of pandemics. On the positive side, the existing scheme in Spain seems to be positive in that

¹⁴²⁸ Nogueira López, Alba and Doménech Pascual, Gabriel, "*Fighting COVID 19...*", op.cit. p.1.

¹⁴²⁹ Nogueira López, Alba and Doménech Pascual, Gabriel, "*Fighting COVID 19...*", op.cit. p.1.

¹⁴³⁰ Malik, Shahnawaz; Mahmood-ul-Hassan, and Hussain, Shahzad (2006) "Fiscal decentralisation and economic growth in Pakistan", *The Pakistan Development Review*, pp. 845-854.

regards, as it combines both way of handling pandemics, for the time being, by established coordination mechanisms¹⁴³¹, as the central government in Spain establishes overarching health policies, but the day-to-day management and delivery of healthcare services are largely decentralized to the regional governments.

In addition, as another part of the assessment, we should also mention the role of Law 33/2011, of 4 October, LO 3/1986, of 14 April, which is other important law in the country on health management issues. Both regulations exclusively pertain to the domain of health protection, as acknowledged by the Spanish Constitution¹⁴³². They do not broaden their provisions to encompass other domains or regulate additional rights that might be impacted by a global health crisis of the magnitude of Covid-19. Moreover, neither of these rules explicitly stipulates any restriction on fundamental rights or outlines the involvement of Parliament, specifically the Congress of Deputies. This applies to both the initial declaration of the state of alarm by the Government and the required approval of subsequent extensions by the Congress.¹⁴³³ To add more specifics on that, while describing all of the necessary measures set out in the General Law on Public Health and L.O. 3/1986, the law provided extremely significant approach to mitigate these concerns on mandatory safeguards by setting out that all preventive measures contained in this legislation must comply with the following principles, preference for voluntary collaboration with health authorities,

¹⁴³¹ Bosch, Xavier (2002) "Spain decentralises its healthcare system.(news roundup)." *British Medical Journal*, vol. 324, no. 7329, pp.68-69, p.68.

¹⁴³² Article 43 of the Spanish Constitution: "Derecho a la Salud",

- " 1. Se reconoce el derecho a la protección de la salud.
2. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La ley establecerá los derechos y deberes de todos al respecto.
3. Los poderes públicos fomentarán la educación sanitaria, la educación física y el deporte.

Asimismo facilitarán la adecuada utilización del ocio"

¹⁴³³ See the Report of Venice Commission (European Commission For Democracy Through Law), Venice Commission - Observatory on emergency situations, section 3.

mandatory measures that entail risk to life cannot be ordered, health limitations must be proportionate to the purposes pursued in each case, and the measures that least harm the principle of free movement of people and goods, freedom of business and any other affected rights must be used.¹⁴³⁴ Hence, as seen the approach brought by the General Law on Public Health, i.e., Law 33/2011, and L.O. 3/1986, is way less restraining, which is positive, but at the same time more on high level again, therefore not tailored to the pandemics, and conditions of our era.

Similarly, Law 33/2011 aims to attain and sustain the utmost standard of health for the population. Its specific goal is to establish the groundwork for reaching and sustaining the highest possible level of people's health. This involves the implementation of policies, programs, services, and various actions by public authorities, businesses, and citizen organizations. The objective is to address the key processes and factors influencing health, thereby preventing diseases and safeguarding and enhancing the health of individuals and communities on both an individual and collective level, as per its language provided.¹⁴³⁵ From our perspective, it is again useful in a way that provides certain foundations in order to fulfill the mandate outlined in Article 43 of the Spanish Constitution and, consequently, to strive for and uphold the utmost standard of public health, our objective is to deliver a comprehensive and up-to-date response, as also clearly stated by the law itself.¹⁴³⁶ In other

¹⁴³⁴ Article 28 of the General Law on Public Health

“ Todas las medidas preventivas contenidas en el presente capítulo deben atender a los siguientes principios:

- a) Preferencia de la colaboración voluntaria con las autoridades sanitarias.
- b) No se podrán ordenar medidas obligatorias que conlleven riesgo para la vida.
- c) Las limitaciones sanitarias deberán ser proporcionadas a los fines que en cada caso se persigan.
- d) Se deberán utilizar las medidas que menos perjudiquen al principio de libre circulación de las personas y de los bienes, la libertad de Empresa y cualesquiera otros derechos afectados”

¹⁴³⁵ See the Report of Venice Commission (European Commission For Democracy Through Law), Venice Commission - Observatory on emergency situations, section 3.

¹⁴³⁶ Article 28 of the General Law on Public Health.

words, it is crucial for public administrations to play a vital role in establishing a regulatory framework that optimizes the level of health while safeguarding other social goods that contribute to the overall well-being of the population. Having said that, again, it only sets out a single sentence on pandemics by stating that the health authority, in coordination with the labor authority, will carry out the following actions in addition to those already established by regulation will implement coordination mechanisms during pandemics or other health crises, particularly for the advancement of preventive measures, and vaccination actions, which we find extremely undetailed for any specific action or safeguard to be provided within the scope of pandemic case scenarios, similar to L.O. 3/1986.

In addition to those two laws, as also listed above, the third most relied law is Act 14/1986, of 25 April on General Health¹⁴³⁷, whose purpose is the general regulation of all actions that allow the right to health protection recognized in Article 43 and related articles of the Constitution to become effective. As per the Law, Spanish citizens and foreign citizens who have established their residence in the national territory are entitled to the right to health protection and health care.¹⁴³⁸ The fundamental goal of the Law is to reform the existing healthcare system, which targets to definitively support the formulation of this General Health Law, by recognizing certain articles of Spanish Constitution, namely, article 43¹⁴³⁹ and article 49¹⁴⁴⁰ of its fundamental regulatory text of the right of all citizens to health protection, a right that, to be effective, requires public powers to adopt appropriate measures. Also, Act 14/1986, of 25 April on General Health, with even greater impact at the organizational level, is the institutionalization, based on the

¹⁴³⁷ For the full Law see Ley 14/1986, de 25 de abril, General de Sanidad.

¹⁴³⁸ Article 1 of Ley 14/1986, de 25 de abril, General de Sanidad.

¹⁴³⁹ Article 43 of the Spanish Constitution.

¹⁴⁴⁰ See Article 49 of the Spanish Constitution: Apoyo estatal para personas con discapacidades,

“Los poderes públicos realizarán una política de previsión, tratamiento, rehabilitación e integración de los disminuidos físicos, sensoriales y psíquicos a los que prestarán la atención especializada que requieran y los ampararán especialmente para el disfrute de los derechos que este Título otorga a todos los ciudadanos”.

provisions of title VIII of our Constitution, of Autonomous Communities throughout the territory of the State, to which their Statutes have recognized broad powers in Health matters. Therefore, in summary, although the law aimed to revolutionize the healthcare system by emphasizing constitutional rights of the citizens and residents, some of which is within the remit our study as described below, it did not touch the sphere of pandemics at all, which again obliges authorities to implement the necessities set out therein only by applying necessary interpretation.

Hence, we believe that a law that is specifically devoted pandemics with the type and duration of any kind of restrictions or suspensions of the fundamental rights foreseen thereunder is vital for the establishment of legal foundations and clarity of legal perspective during pandemic. For instance, in a statement issued on April 24, 2020, the UN Human Rights Committee (HRC), tasked with overseeing States' adherence to the ICCPR, suggested that instead of resorting to complete suspensions of certain rights through derogations, restrictions on freedom of movement and assembly could be sufficient to achieve public health and other objectives associated with containing the pandemic. The committee emphasized that entirely suspending specific rights might lead to disproportionate hardships for individuals, particularly if there are no mechanisms in place for a personalized evaluation of the impacts of such derogations.¹⁴⁴¹ It therefore, from our perspective, requires pre-defined rules which states to-do and not-to-dos during any pandemic scenarios during pandemic circumstances, rather than high level descriptions which may end up in ambiguity of the terms. Within the similar vein, the vagueness of these laws is also criticized by Dolores Utrilla, Manuel Antonio García-Muñoz, Teresa Pareja Sánchez that are generic and broad, empower health authorities to undertake 'any necessary measure' to address health emergencies, contingent upon the principle of proportionality¹⁴⁴² For example,

¹⁴⁴¹ Geneva Center of Humanitarian Studies (2022) "Emergencies and human rights in times of COVID-19", available at: <https://humanitarianstudies.ch/emergencies-and-human-rights-in-times-of-covid-19/> (accessed on 23 June 2024).

¹⁴⁴² Utrilla, Dolores; García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) "Spain: Legal Response...", op.cit. p.4.

Article 26 of Law 14/1986 stipulates that in the presence of an imminent and extraordinary health risk or when reasonably suspected, health authorities are empowered to implement preventive measures they deem necessary¹⁴⁴³. These measures may include the confiscation or immobilization of products, suspension of certain activities, closure of businesses or their facilities, intervention with material and personal resources, and any other measures justified from a health perspective.¹⁴⁴⁴

Accordingly, we still believe that although it creates the required legal foundation for any required safeguards to be implemented to save people lives, which is very much important for right to life of individuals, it seems a bit abstract when it comes to pandemic specific restrictions, as there is not any specified references on pandemic case scenarios, which might be different than other public health problems by its nature. Suitably, on this very topic, on May 24, 2021, the Spanish Supreme Court (Tribunal Supremo)¹⁴⁴⁵ delivered a judgment (in Cassation Appeal Number 3375/2021), providing the first clarification on the crucial matter of utilizing pre-existing Spanish public health legislation in the context of the ongoing Covid-19 pandemic. This judgment addressed the question of whether and how such legislation could be invoked for the implementation of preventive measures that entail restrictions on fundamental rights. On the healthcare side, we are of the view that it surely would help to some degree. On the other hand, to move even further, to the extent it is relevant to the main discussion of this thesis, namely data protection law and contact tracing activities, our evaluation on the topic is that there is already inherent risk of implementing an outdated law, given that these laws were passed almost forty years ago. It, thus, means that it is not precisely covering the new type of concerns resulted on fundamental rights of individuals. In other words, now the list of fundamental rights might

¹⁴⁴³ Part III of Ley 14/1986, de 25 de abril, General de Sanidad.

¹⁴⁴⁴ Utrilla, Dolores; García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) "Spain: Legal Response... ", op.cit., p.5.

¹⁴⁴⁵ For the structure of Tribunal Supremo in general, see <https://www.poderjudicial.es/cgpi/es/Poder-Judicial/Tribunal-Supremo/> (accessed on 6 October 2023).

be interpreted differently and more broadly than as it used to be with regards to the right to privacy of individuals living in society. In more detail, as discussed by Servet, Covid situation, in which the ease of coronavirus contagion was not only challenging the entire healthcare system but the entire state in general, requires all forms of business, administrative, and citizen support to combat the easy spread of this virus.¹⁴⁴⁶ To this end, again, our approach is more in favor of legislative act that comprises more of the impacted fundamental rights.

Obviously, we are not alluding to design and implement a legislation, which prioritizes privacy of individuals, rather than the management of public health, but instead, what we offer is, in line with the general stand of this thesis, to consider different aspects of restriction on fundamental rights in light of the new era, while providing preventive measures in the society against any type of Pandemic. The underlying reason of our proposal is, at first glance, it appears reasonable to anticipate that States' responses to the COVID-19 pandemic would involve the use of derogations, given that the pandemic aligns well with the characteristics of a public emergency.¹⁴⁴⁷ Especially when considering the elevated rates of hospitalization resulting from the new coronavirus, there have been significant challenges and, in some cases, the outright collapse of healthcare systems in various regions of Spain¹⁴⁴⁸. This has had detrimental effects on individuals infected with Covid-19 as well as others in need of medical care.¹⁴⁴⁹ Also, the economic repercussions of the pandemic have contributed to a surge in unemployment rates across various

¹⁴⁴⁶ Servet, Vicente Magro (2020) "El reproche penal a los actos de desobediencia a agentes de la autoridad en el período de Estado de Alarma por el Coronavirus." *Diario la ley*, vol. 9606, 2, pp.1-15, p.2.

¹⁴⁴⁷ Geneva Center of Humanitarian Studies (2022) "Emergencies and human rights in times of COVID-19", para 5.

¹⁴⁴⁸ Particularly, Catalonia, Madrid and Andalucia, as per the data provided on Statista Website, Número de casos confirmados de coronavirus en España a fecha de 30 de junio de 2023, por comunidad autónoma <https://es.statista.com/estadisticas/1100641/regiones-afectadas-por-el-covid-19-segun-los-casos-confirmados-espana/> (accessed on 24 June 2024).

¹⁴⁴⁹ Geneva Center of Humanitarian Studies (2022) "Emergencies and human rights in times of COVID-19", para 5.

countries, including but not limited to Spain as well, jeopardizing other fundamental rights such as the right to housing and access to adequate food. Accordingly, new type of pandemics would augment the number of rights impacted due to its prevalent nature. Furthermore, such necessity of revamping the law would also be a trigger point to enhance entire public healthcare structure, as proposed by the study of Mancebo Lozano, which simply asserts that Covid-19 crisis could be a turning point to update the existing system.¹⁴⁵⁰ Mancebo Lozano's reasoning is, there have been significant differences, focused on the difficulty of coordination between territories. The transfer of management competencies for public service provision, carried out with the formation of the different autonomous health services, has resulted in a gap in the unidirectional strategy in national health policies.¹⁴⁵¹ There is a lack of connectivity between the general strategy, centrally focused on overall public action objectives, and the management competencies of public services.¹⁴⁵² Hence, we believe that, such consolidated new legislation could strictly bolster the ability of country to respond more solidly to the pandemic scenarios as well.

Therefore, in order to mitigate such concerns, as also being subject broad consensus by both scholars and courts, which were detailed above, it is important to modernize the legislation and be more specific with the accountabilities and responsibilities of governments, and restrictions of other important rights that might be impacted from the pandemic as well. Correspondingly, while calling out the importance of modernizing the existing legislation, our assessment on the topic is that there is automatically another dimension of the issue, which is in line with the topic of our research topic, namely consideration of personal data protection of individuals in society as well. To give more specific example, for instance, as indicated by Charter of

¹⁴⁵⁰ For the full article see Mancebo Lozano, Esteban (2021) "El estado de bienestar y la nueva gestión de los servicios públicos en España y Latinoamérica: innovación en los servicios sociales y sanitarios tras el Covid-19" *Saber Servir: Revista de la Escuela Nacional de Administración Pública*, vol. 6, pp. 95-121.

¹⁴⁵¹ Mancebo Lozano, Esteban (2021) "El estado de bienestar y la nueva gestión ..., *op.cit.*, p.97.

¹⁴⁵² Mancebo Lozano, Esteban (2021) "El estado de bienestar y la nueva gestión ..., *op.cit.*, p.98.

Fundamental Rights of the European Union¹⁴⁵³, it and detailed in the Data Protection in Spain section of this Chapter that, protection of personal data is evidently a fundamental right of individuals. As stated by Council of Europe that in addition to emphasizing that data protection cannot in any way stand in the way of efforts to save lives, it is critical to reiterate that the exercise of human rights, including those related to privacy and data protection, is still valid.¹⁴⁵⁴ Therefore, we propose to inclusion of personal data protection related articles in the newly formed legislation that is to be tailored to the pandemic and healthcare risks. To some extent, the LO 3/1986 articulates the significance of respecting right to privacy during the implementation of the relevant safeguards¹⁴⁵⁵, which we find quite pleasant from data protection and privacy perspective. However, as also concluded by Vicente Díaz and Callejo Carrión that the discussion might not be solely about the risk of violating rights like privacy or data protection, but rather whether authorities are fulfilling their obligation to adopt necessary measures to protect the right to life and health.¹⁴⁵⁶ To this end, we believe that there is a close relationship between these fundamental rights impacted by the pandemic, by their nature, both of which must be reflected onto the new type of pandemic law.

Suitably, the main reason of our proposal for the inclusion of new type of rights into the scope of more specific new law is that, due to the novelties of our era, right now it is important to keep the secrecy and confidentiality of health related data of individuals, which is deemed as sensitive personal data under the GDPR and Spanish Data Protection Law ("Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos

¹⁴⁵³ Article 8 of the Charter of Fundamental Rights of the European Union, "Right to respect for private and family life, home and correspondence" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

¹⁴⁵⁴ See Council of Europe, Covid 19 and Data Protection <https://www.coe.int/en/web/data-protection/covid-19-data-protection> (accessed on 23 June 2024).

¹⁴⁵⁵ See Article 10 of Organic Law 3/1986, of April 14, on Special Measures in Public Health Matters <https://www.boe.es/buscar/act.php?id=BOE-A-1986-10498>.

¹⁴⁵⁶ Vicente Díaz, Matilde and Callejo Carrión, Soraya (2021) "On alarms, geolocations and rights: Regarding a regulation that is more than dangerous for fundamental rights." *CEFLegal. Practical Law Review*, pp.109-142, p.141.

digitales or “L.O 3/2018”) as well. The main reason of our approach can also be found in the words of Nieto Garrido, who provided that Law on Special Measures on Public Health Matters was passed in 1986, the fundamental right to safeguard personal data did not exist as a separate right.¹⁴⁵⁷ That's why the current legislature has chosen to demand a specific law for handling personal data in situations necessitated by public interest within the domain of public health (e.g., as stated in Article 9.2 of Law 3/2018). To this end, to tackle such risks, sacrificing right to privacy has also become more serious and relevant, compared to forty years ago because of advanced techniques in cyber-crimes and personal data breaches. As such, we believe that reformed more specific healthcare law with inclusion of certain considerations on extension of the scope of fundamental rights, including but not limited to right to privacy, would significantly contribute to the ambiguity in the legal landscape of Spain for any potential pandemic or infectious diseases related scenarios again. To this end, a supportive of our approach, such necessity was also caveated by the study of Nieto Garrido.¹⁴⁵⁸ which we find extremely in line with our current stance. Nieto Garrido addressed the matter that the generic authorization outlined in Article 3 of Law 3/1986, dated 14 April, focusing on Special Measures regarding Public Health, did not suffice. At the time of enacting the Law on Special Measures concerning Public Health in 1986, the fundamental right to personal data protection did not exist independently.¹⁴⁵⁹ Consequently, the current legislature deems it necessary to mandate a specific law for processing personal data concerning public health reasons (as seen in Article 9.2 of L.O. 3/2018). Such a law can also lay down further prerequisites concerning security and confidentiality. Thus, in line with this

¹⁴⁵⁷ Nieto Garrido, Eva María (2021) "Risks for the fundamental right to the protection of personal data stemming from the COVID-19 sanitary crisis: A Spanish perspective.", *Freedom, Security & Justice: European Legal Studies*, ISSN-e 2532-2079, *Rivista quadrimestrale on line sullo Spazio europeo di libertà, sicurezza e giustizia*, n. 1, pp. 197-218, p.211.

¹⁴⁵⁸ For the full study see Nieto Garrido, Eva María (2021) "Risks for the fundamental right to the protection of personal data stemming from the COVID-19 sanitary crisis: A Spanish perspective.", *Freedom, Security & Justice: European Legal Studies*, ISSN-e 2532-2079, *Rivista quadrimestrale on line sullo Spazio europeo di libertà, sicurezza e giustizia*, n. 1, pp. 197-218.

¹⁴⁵⁹ Nieto Garrido, Eva María (2021) "Risks for the fundamental right...", *op.cit.*, p.281.

direction, as mentioned, while on the positive side Act 33/2011, of 4 October on public health articulates the significance of respecting right to privacy during the implementation of the relevant safeguards¹⁴⁶⁰, there are not any personal data protection or privacy reference made by the other laws, which obliges us to consider a solution. Therefore, we believe that it would still be required to update these necessities in light of the current technological and healthcare related challenges as well. Thus, while repairing and updating the deficient parts of the existing healthcare laws, namely Public Health Special Measures Act, Article 26 of the General Healthcare Act, and Article 54 of the General Public Health Act, it would also provide more in depth aspects on other important rights of individuals that are impacted by the nature of pandemics and technological challenges at the same time. Having said that, it is still important to remind the main necessities that were discussed in the previous section for restrictions.

3. Legal Orders on Asistencia Covid and Radar Covid

Following to Decreto de Alarma, the Secretary of State for Digitalization and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation (“SEDIA”) was tasked with developing various actions for the management of the health crisis brought on by the Covid-19, carrying out various actions aimed at improving the management of the crisis, in Order SND/297/2020 (“the Order”), of 27 March, issued by the Ministry of Health.¹⁴⁶¹ This directive, among other things, calls for the creation of technology solutions and mobile applications for data collecting in order to enhance the operational effectiveness of health services and to offer individuals with better

¹⁴⁶⁰ Article 10 of Organic Law 3/1986, of April 14, on Special Measures in Public Health Matters <https://www.boe.es/buscar/act.php?id=BOE-A-1986-10498>.

¹⁴⁶¹ Order SND/297/2020, of March 27, entrusting the Secretary of State for Digitization and Artificial Intelligence, of the Ministry of Economic Affairs and Digital Transformation, with the development of various actions to manage the health crisis caused by COVID-19, available at: <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-4162>.

care and accessibility.¹⁴⁶² The order, SND/297/2020, has since been issued with the aim of digitalizing and accelerating various administrative processes related to the health crisis.¹⁴⁶³ It therefore, led to the creation of a self-evaluation app that simply uses location information to confirm whether the user is in their home province.¹⁴⁶⁴ More specifically, within the scope of this Order, the Ministry of Health ordered the development of two analysis tools: “Asistencia COVID-19”, whose main features will be discussed in the next Chapter in detail, which is, in short, focused on linking and combining data from mobile operators, in an aggregated and anonymized way, with the aim of analyzing the mobility of people prior to and during confinement.¹⁴⁶⁵ The data controller is the National Statistics Institute (Instituto Nacional de Estadística).¹⁴⁶⁶ We briefly wanted to introduce the app and mention the general information as background for the following parts, but more importantly, following to the order, there were two resolutions passed, which are respectively Resolution of April 30, 2020, of the General Secretariat of Digital Administration, by which the Agreement between the SEDIA and Telefónica Digital España, SLU, for the operation of the AsistenciaCovid19

¹⁴⁶² Rodríguez Ayuso, Juan Francisco (2020) "Compliance with the regulations on personal data protection in a state of alarm by Public Administrations", Faculty of Law and Administration of the Jagiellonian University, Law Against Pandemic, available at: <https://lawagainstpandemic.uj.edu.pl/2020/05/20/compliance-with-the-regulations-on-personal-data-protection-in-a-state-of-alarm-by-public-administrations/> (accessed on 23 June 2024).

¹⁴⁶³ Mieza, Unai (2021) “How Health And Location Data Were Handled In Times Of Covid-19”, Lozano Schindhelm SLP, <https://es.schindhelm.com/en/news-jusful/covid-19-unit/how-health-and-location-data-were-handled-in-times-of-covid19-e168040> (accessed on 23 June 2024).

¹⁴⁶⁴ Mieza, Unai (2021) “How Health And Location Data Were Handled In Times Of Covid-19”, Lozano Schindhelm SLP, <https://es.schindhelm.com/en/news-jusful/covid-19-unit/how-health-and-location-data-were-handled-in-times-of-covid19-e168040> (accessed on 23 June 2024).

¹⁴⁶⁵ Resolución de 8 de mayo de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Comunidad Autónoma de Castilla-La Mancha, sobre la adhesión al uso de la Aplicación AsistenciaCOVID19, («BOE» núm. 150, de 27 de mayo de 2020, páginas 35080 a 35099 (20 págs.)), Terceros.

¹⁴⁶⁶ Article 2 of the Order SND/297/2020, DataCovid-19: Estudio De La Movilidad Aplicada a la Crisis Sanitaria.

application in the context is published of the health crisis situation caused by COVID-19, which dealt with the design and creation of the referenced application in the Order SND/297/2020,¹⁴⁶⁷ and the Resolution of October 13, 2020, of the Undersecretariat, by which the Agreement between the Ministry of Economic Affairs and Digital Transformation and the Ministry of Health is published, regarding the Radar Covid application¹⁴⁶⁸, which we will also review and analyze in this section from data protection perspective.

To begin with, the Order provided that the National Statistics Institute (“INE”)¹⁴⁶⁹ would get anonymized location data from mobile phone users, which will allow researchers to examine where people were prior to and during an alert state. This is actually like the lawful basis discussions detailed in this Chapter. However, the reason we wanted to discuss this here is that such purpose is provided because of the Order. From our perspective, compatible with the previous discussions held in the previous chapters, despite the anonymized nature of data at stake, still it might raise concerns in the eyes of data subjects, as it is being used by the government for the surveillance of activities that happened before and after an alert state, which might still be subject to misuse. Accordingly, it should have been clearly indicated as an update to the privacy policy of the contact tracing application, and notified to data subjects via several public information campaigns as part of the transparency acts targeted via article 5 of the GDPR.¹⁴⁷⁰ Although not exactly the same, but somehow similar type of action took place, as the government sent text messages to the individuals that “all information will be collected for purposes strictly in the public interest in the field of public health, and in the face of the health emergency decreed, in order to protect and safeguard an essential interest in people’s lives, in the terms described in this privacy

¹⁴⁶⁷ BOE núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829.

¹⁴⁶⁸ BOE núm 273, 15 de octubre de 2020, BOE-A-2020-12339.

¹⁴⁶⁹ For more details on the structure of Instituto Nacional de Estadística <https://www.ine.es/> (accessed on 23 June 2024).

¹⁴⁷⁰ Article 5-1-a of the GDPR, principles relating to the processing of personal data, lawfulness, fairness and transparency.

policy”.¹⁴⁷¹ However, it is still not clear enough to reduce the amount of concerns raised due to the use of geolocation data by Asistencia application, which will be detailed in the following chapter as well. On the top of that, what is more concerning is that "until how many days before" it could be geolocated is not mentioned, which leads to legal ambiguity.¹⁴⁷² Therefore, the Order stated that the application would allow the geolocation of the user for the sole purpose of verifying that the user is in the autonomous community in which they declared to be, yet it did not specify any limit nor condition thereupon.¹⁴⁷³

The Order also set out a very significant matter from data protection standpoint, which was rightly subject to many challenges from AEPD, as it will be detailed in the next Chapter, which is the identity of the controller of the application to be developed. Considering that Order did set out that the provisions of the Order must be provided as interpretation without prejudice to the application of the regime provided GDPR and Ley Orgánica 3/2018,¹⁴⁷⁴ on a high level, it should not be extremely surprising to see privacy friendly approaches from the regulator. However, even more than that, from the very beginning, the Ministry of Health and SEDIA indicated the allocation of responsibilities among themselves as part of the arrangement for the implementation of the application. To this end, in order to articulate this clear distinction, the Order provided that the person in charge of the treatment will be the Ministry of Health and the person in charge of the treatment and owner of the application will be the General Secretariat of Digital Administration.¹⁴⁷⁵ The Ministry of Health, as data controller, authorizes the

¹⁴⁷¹ See Díaz, Efrén (2021) “Geolocation Apps Do not Cure Covid-19 They Analyze Peoples Mobility”, Geospatial World, available at: <https://www.geospatialworld.net/article/geolocation-apps-do-not-cure-covid-19-they-analyze-peoples-mobility/> (accessed on 23 June 2024).

¹⁴⁷² Díaz, Efrén (2021) “Geolocation Apps Do not Cure Covid-19 They Analyze Peoples Mobility”, Geospatial World, available at: <https://www.geospatialworld.net/article/geolocation-apps-do-not-cure-covid-19-they-analyze-peoples-mobility/> (accessed on 23 June 2024).

¹⁴⁷³ Order SND/297/2020, First Part.

¹⁴⁷⁴ Article 12 of the Order SND/297/2020, Régimen de Protección de Datos, Seguridad y Confidencialidad.

¹⁴⁷⁵ Order SND/297/2020, First Part.

General Secretariat for Digital Administration to resort to other managers in the execution of the provisions of this section. We believe that the approach on theory was positive. However, as detailed in Chapter 7, it resulted in plenty of ambiguities, once other institutions stepped in the process, which alleviated the discussions around clarity of data controller and processor roles. Therefore, from that perspective, the Order should have clearly indicated each designated institutions with clear explanations and roles. In addition to this, the Order also indicated an interesting part, which was not provided in most of the EEA states. This is related to entrusting the SEDIA with the development of a conversational assistant/chatbot to be used via WhatsApp and other instant messaging applications. It provided official information when asked by the public. The design was based on official information from the Ministry of Health. This application also implemented for certain time. Accordingly, like the approach provided again the contact tracing applications, the Order did not differ its approach from the identity of data controller though. As said the order indicated the person responsible for the treatment will be the Ministry of Health and the person in charge of the treatment and owner of the chatbot will be the SEDIA through the General Sub-directorate for Artificial Intelligence and Digital Enabling Technologies ¹⁴⁷⁶. Hence, from our perspective, it is possible to leverage the discussions around the identity of controller raised by AEPD into this area as well. That being said, we do not think that these defected parts should shadow the other positive things established by the Order itself.

Subsequently, another crucial topic was delineated by the Order, which we believe worth discussing from data protection standpoint that it was provided by the order SEDIA was entrusted, by the Ministry of Economic Affairs and Digital Transformation, following the model undertaken by INE, in its mobility study called Data Covid fed by Covid Asistencia application and the crossing of data from mobile operators, in an aggregate manner and anonymous, the

¹⁴⁷⁶ For the further details on Strategic Action Digital Economy and Society see Ministerio de Transformacion Digital <https://sedediatid.mineco.gob.es/en-us/procedimientoselectronicos/Paginas/detalle-procedimientos.aspx?IdProcedimiento=2> (accessed on 23 June 2024).

analysis of the mobility of people in the days before and during confinement. The competent State Secretariat reassured that compliance with the GDPR and L.O. 3/2018 would be ensured.¹⁴⁷⁷ All data collected within the scope of data analysis through Asistencia App collected in an aggregated and anonymous manner by the INE has been made available to the governments of the Autonomous Communities. Mobile phone location data was used to track people's movements and verify how closely a nationwide lockdown was being respected.³⁵ Information helped enable verification that users' area of residence match their actual location, thus enabling measurement of compliance with containment measures. The project was based on data provided by the main telecommunications operators, yet Data received from these operators did not include personal data.

Having said that, we are still of the view that considering the controversial nature of the Decreto de Alarma and other incumbent health regulations due to aforementioned aspects, as a bit of caution, the Order seemed to take more diligent approach by prioritizing the main principles of the GDPR for its applicability on this specific purpose. Thus, the Order emphasized that in the execution of this data driven study, compliance with the provisions of the GDPR, and Ley Orgánica 3/2018.¹⁴⁷⁸ Conversely to the previous samples on the controllers, this time the data controller of this activity was selected as INE, and from our perspective, it is important indicator to reiterate the responsibility of INE for the implemented processing activities within the scope of the mobility program.

Furthermore, as per the Order those in charge of the treatment would be the mobile electronic communications operators, with whom an agreement is reached. INE, as data controller, authorized the operators to resort to other managers in the execution of the provisions of this section. However, it is still concerning in many aspects given INE has concluded that, in general, since the state of alarm was adopted, 85% of people did not move from their area

¹⁴⁷⁷ García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain...." op.cit. para 11.

¹⁴⁷⁸ See Article 4 of the Order SND/297/2020, personal data protection.

of residence, which is a clear indication of the visibility on people's movements, later will be addressed in Chapter 7. The Data COVID mobility study¹⁴⁷⁹, allowed an estimate of the mobility of the Spanish population during the period of application of the containment measures in relation to a normal situation. Like this study, the Government later announced another study to be run by the Spanish National Scientific Research Council (CSIC). The research team used mobile data obtained by telecommunication operators to study the effectiveness of lockdown measures.¹⁴⁸⁰ However, the second one was not fed by the Asistencia Covid application, therefore, did not raise a concern within the scope of this Order.

Nonetheless, regarding the part concerning to our study, our evaluation on the topic is that despite the certain criticisms against the application itself which will be later delineated in Chapter 7, and guarantees provided by the Government in return, it still seems like huge portion of the society was somehow tracked, which might be still subject to concerns delineated in Chapter 2. Furthermore, given that such mobility was implemented because of obligatory act, which is not really in line with the general approach of European Union as detailed in voluntariness of the applications sections. Correspondingly, despite such potential concerns, the Order did not specify the limits of such obligation, and the content of such guarantees for fundamental rights of users of those applications mentioned. We understand that such Order might not contain all details, rightly, yet, in general, there is mostly a few more general statements which would point out more specific regulations, in such kind of Orders due to their nature. Or similarly, AEPD could also provide a more detailed approach on geolocation data; the same was reiterated by Vicente Diaz and Callejo Carrión: nothing was mentioned about the potential monitoring that might occur based on the extensive powers

¹⁴⁷⁹ For the further details of the study see Ministerio de Transportes y Movilidad Sostenible, "Studio de movilidad con Big Data durante la pandemia" <https://www.mitma.gob.es/ministerio/covid-19/evolucion-movilidad-big-data> (accessed 19 June 2024).

¹⁴⁸⁰ Aszodi, Nikolett; Galaski, Jascha; Konoplia, Oleksandra and Reich, Orsolya (2021) "COVID-19 Technology in the EU: A Bittersweet Victory for Human Rights." Civil Liberties Union for Europe: Berlin, Germany, pp.1-77, p.45.

granted to health authorities in this exceptional epidemic situation, which even includes restricting people's freedom of movement.¹⁴⁸¹ Nonetheless, we still do not entirely want to bombard it with harsh criticisms as it at least pointed out the data protection laws in place for the activities that were undertaken within the scope of the Order, as touched based above. We are, therefore, of supportive of what provided by Domínguez Álvarez that the treatments mentioned in Order SND/297/2020 should adhere to a legitimate basis, as will be discussed below.¹⁴⁸² These data processing activities must uphold specific principles safeguarding personal data, including but not limited to purposefulness, security, data minimization, and restrictions on retention periods.¹⁴⁸³ Similarly, we believe that what De la Cruz Mena stated on this regards, more specifically on Big Data collection, seems to be really useful and compatible with our proposal as well. They provided that while Big Data is one of the primary tools receiving significant government investment and is proving to be effective, these extremely sensitive data being collected under a law where rights are suspended can be dangerous, not necessarily due to their current use but due to a potential scenario where, even when the pandemic is nearly controlled, the collection of people's geolocations continues, deviating from the initial.¹⁴⁸⁴ Thus, in an ideal scenario, Big Data should be handled solely for its initial purpose, completely anonymized, and with users being fully aware of the information they're providing as well, not to be subject to risk of data being disclosed to external third parties.¹⁴⁸⁵ As such, we can easily provide that such approach has been in line with our stance

¹⁴⁸¹ Vicente Díaz, Matilde and Callejo Carrión, Soraya (2021) "On alarms, geolocations and rights: Regarding a regulation that is more than dangerous for fundamental rights." *CEFLegal. Practical Law Review* pp.109-142, p.141.

¹⁴⁸² Domínguez Álvarez, José Luis (2020) "Public Administration's Challenges in Order to Guarantee the Fundamental Right of Personal Data Protection in the Post-COVID-19 Era.", *Revista Eurolatinoamericana de Derecho Administrativo*, vol. 7, núm. 1, pp. 167-191, p.178.

¹⁴⁸³ Domínguez Álvarez, José Luis (2020) "Public Administration's Challenges...", *op.cit.*, p.175.

¹⁴⁸⁴ de la Cruz Mena, Víctor (2020) "Implicacions ètiques del big data en la sanitat pública", *Universitat Autònoma de Barcelona, Dipòsit Digital de documents de la UAB de la* <https://ddd.uab.cat/record/231494> (Accessed on 8 June 2024), p.7.

¹⁴⁸⁵ *Ibid.*, p.7.

against importance of technical and organizational measures through the Chapters as well.

Subsequently, within the scope of the Order, certain significance was attributed to the coordination mechanism, which we find positive indeed. More specifically, SEDIA was entrusted by the Ministry of Economic Affairs and Digital Transformation, with the creation of a central coordination point for the evaluation of other technological proposals by other organizations and entities. Interesting enough, the Order also set out that the execution of the measures that are contemplated therein will not imply any cost for the Ministry of Health. Therefore, there were many debates around the cost incurred by the SEDIA, but no one seemed to raise any criticism regarding the cost incurred by Ministry of Health. Our evaluation on this approach is that as per the legal perspective the notion of being data controller, or joint controllers could mean to be in charge for many other aspects of the processing activities.¹⁴⁸⁶ Although, it does not cover the monetary obligations, we believe that determining many aspects of the processing activities is not really compatible with leaving everything to another party. This is the one of the key discussions regarding the controller and processor debates in general. On the positive side, beyond all of these features and discussions, in case anything goes wrong in terms of legal and data protection point of view, the Order clearly set out that against the Order, a contentious administrative appeal may be filed within a period of two months from the day of its publication, before the Contentious-Administrative Chamber of the Supreme Court¹⁴⁸⁷, in accordance with the provided in article 12 of Law 29/1998, of July 13,

¹⁴⁸⁶ See Article 1 of Order SND/297/2020, Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

¹⁴⁸⁷ For the further details of Contentious-Administrative Chamber of the Supreme Court and the associated Process see https://www.poderjudicial.es/portal/site/cgpj/menuitem.65d2c4456b6ddb628e635fc1dc432ea0/?vgnextoid=44fb2daed2278510VgnVCM1000006f48ac0aRCRD&vgnnextchannel=6326e44797678510VgnVCM1000006f48ac0aRCRD&vgnnextfmt=default&vgnnextlocale=en&lang_chosen=en (accessed on 16 October 2023).

regulating the Contentious-Administrative Jurisdiction.¹⁴⁸⁸ Therefore, we are of the view that establishing such corrective instrument against the validity of the acts implemented by the Government within the scope of this Order is significant and in line with the spirit of rule of law and right to privacy. In other words, it gives a break mechanism for the driver, in case the car will have risk of crash.

Following to dealing the nuances of the Order, we would like to deep dive into the features of the of the Resolution of April 30, 2020, of the General Secretariat of Digital Administration, by which the Agreement between SEDIA and Telefónica Digital España, SLU, for the operation of the Asistenciacovid19 Application in the context is published of the health crisis caused by COVID-19. First, it is positive the observe the allocation of accountabilities and responsibilities between data controller, processor and sub-processor is quite detailed and strict, which we find in line with the spirit of the GDPR and Ley Orgánica 3/2018 law in general, given that any room for arbitrariness of abusiveness of data processor and sub-processor of this applications was mitigated by this Order's diligent articles. To provide a more detailed example, specifically, both the data Processor and Sub-processor are obligated to inform the Data Controller about any request made to exercise rights such as access, rectification, deletion, opposition, processing limitation, data portability, and to avoid being subjected to individually automated decisions, made by an interested party whose data has been processed by the Processor or Sub-processor in order to comply with the purpose of this Agreement, so that the Data Controller resolves it within the deadlines established by current regulations.¹⁴⁸⁹ Furthermore, the stipulation of an upper limit for the transfer of the request to the Data Controller from processor or sub-processor was limited with the maximum of three business days following receipt of the request by the Data Processor or Sub-processor,

¹⁴⁸⁸ See Article 7 of the Order SND/297/2020, Régimen de recursos.

¹⁴⁸⁹ «BOE» núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4829 .

accompanied by other information that may be relevant to resolve the request.¹⁴⁹⁰ Therefore, our evaluation on such approach is quite positive, considering that there were not any room left for the arbitrary activities that create the main source of concern for these applications in general, which may result in detrimental impacts on data subjects (users).

Additionally, considering these, another positive approach provided by the Ministry is related to the duty of confidentiality, which massively created the center of discussion points. In other words, this agreement was helpful to enforce data processor and sub-processor as much as possible to protect the personal data of data subjects. To be more specific, it was stipulated in the agreement that both parties undertake to maintain the utmost confidentiality and secrecy regarding the information classified as confidential provided by one to the other, because of collaboration in the activities covered by this Agreement. Correspondingly, as per the Resolution of April 30, 2020, confidential information was considered all information and personal data to which the Ministry of Health as Data Controller, the General Secretariat of Digital Administration¹⁴⁹¹ (“SGAD”) as Data Processor and Telefónica as Sub-processor have access, as well as any other party that may participate in the process, development, management or exploitation of the application or services referred to in the Convention. Once the relationship that is the subject of this Agreement has ended, sub-processor will be obliged to delete such data, which is positive indication of duly implementing data destruction duties in line with the storage limitation principles of the GDPR¹⁴⁹² and Organic Law 3/2018¹⁴⁹³. Therefore, we are of view that due to the sensitivity of personal data at stake, there is still level of inherent risk in terms of processing activities, despite the existence of GDPR and Ley Orgánica 3/2018 related provisions

¹⁴⁹⁰ «BOE» núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4829.

¹⁴⁹¹ See the General Secretariat of Digital Administration <https://administracionelectronica.gob.es/pae/Home/en/pae/Organizacion/SGAD.html?idioma=en> (accessed on 16 October 2023).

¹⁴⁹² Article 5-1-e of the GDPR, storage limitation.

¹⁴⁹³ Article 5-1-e of the Organic Law 03/2018, storage limitation.

of the Order.¹⁴⁹⁴ However, we believe that having a reference to the regulations, at least, are efficient factors that indicated that privacy concerns are considered to the some extend, as detailed above. Again, we would like to assess the other bits in isolation, given that controller and processor ambiguity was rightly subject to complaints.

Accordingly, what is satisfying from the data protection point of view is that there are detailed tasks attributed to the vendor company Telefónica for the security of personal data processed as part of the use of the application, which is compatible with our strong emphasis on the significance of technical and organizational measures that needs to be implemented by controllers and/or processors. Lastly, even beyond those technical safeguards, as a contractual security mechanism for the proper implementation of the relevant responsibilities and accountabilities that were set out as part of the agreement, the Resolution of April 30, 2020 provided that in accordance with the provisions of Article 49.1.f) of Law 40/2015, of 1 October, a Monitoring Committee shall be set up for the management, monitoring and control of this Agreement and the commitments made by the signatories.¹⁴⁹⁵ From our perspective, this certainly cemented the proper implementation of the Agreement, and till date, we have not witnessed any feared event or breaching act from none of these parties in this regards, which is important for satisfying the contractual obligations that were undertaken by the Parties, thereby reflecting positively onto the privacy rights of the users.

Following to the details of the Resolution of April 30, 2020, we would like to analyze the nuances of the Resolution of October 13, 2020, of the Undersecretariat, by which the Agreement between the Ministry of Economic Affairs and Digital Transformation and the Ministry of Health is published, regarding the Radar Covid application, which establish the basis agreement for the Radar Covid application, there is also delineation of data controller,

¹⁴⁹⁴ For the details of the GDPR and Ley Orgánica 3/2018 related provisions see article 4 and 7 of the «BOE» núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829.

¹⁴⁹⁵ See Article 13 of the «BOE» núm.125, de 5 de mayo de 2020. BOE-A-2020-4829 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4829 .

processor and sub-processor relationship and attributed responsibilities.¹⁴⁹⁶ Suitably, this approach, as detailed in legal basis of Radar Covid application section, aimed to contribute to the clarity on the role of different public institutions, in line with the transparency and legal basis requirements, but it was also subject to certain reactions from AEPD side from controller and processors perspective, which will be detailed in Chapter 7.

To begin with, the Resolution was created for two fundamental reasons. The first one is to delegate to the SGAD of the Ministry of Economic Affairs and Digital Transformation ¹⁴⁹⁷, all the powers of design, development, implementation, and evolution of the Radar Covid application, and also delegate to the SGAD the power of the Minister of Health to sign collaboration agreements with the communities and autonomous cities for their accession to the use of Radar Covid application. Therefore, as seen broad range of responsibilities and tasks were provided to SGAD as part of this Resolution. We are of the angle that, the law implicitly indicated the underlying reason of such broad range of tasks attributed to SGAD, by calling out the fact that it is of general interest for the signatory parties to respond to the common objective of increasing the effectiveness and efficiency of Public Administrations and establish formulas that contribute to providing a better service to citizens in a matter as sensitive as is the fight against COVID-19.¹⁴⁹⁸ Nevertheless, what is more interesting from our point of view is that SGAD has not been limited with one or two important coordination and design tasks, but also undertook both technical and organizational measures pertaining to the Radar Covid application, including but not limited to obligations necessary for the correct functioning of the application and, especially its integration with the European contact exchange system, including the formal request to join the system and support for the operation of the system and the management

¹⁴⁹⁶ «BOE» núm. 273, de 15 de octubre de 2020, pp. 88391-88398 <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-12339>.

¹⁴⁹⁷ For the detailed structure of the Ministry see <https://portal.mineco.gob.es/en-us/ministerio/Pages/default.aspx> (accessed on 16 October 2023).

¹⁴⁹⁸ Article 11 of the BOE» núm. 273, de 15 de octubre de 2020, pp.88391-88398, “Regimen Juridico”, <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-12339>.

of the associated infrastructure.¹⁴⁹⁹ However, although it seems very diligent to attribute certain tasks to single body, we are of the view that it might result in the lack of capability to implement all of the tasks attributed by the Ministry of Economic Affairs and Digital Transformation and Ministry of Health at the same time, and creates confusion for the role of data controller and processors, as detailed in Chapter 7 within the scope of AEPD decisions on the app.

On the one hand, we understand that such approach aimed to uplift the public trust by indicating the level of seriousness devoted to the implementation of these measures, which will be also detailed below with another aspect, on the other hand it might be detrimental for data protection requirements due to huge amount of technical, organizational, and administrative tasks that were assigned. In other words, it is always risky to leave majority of the significance safeguards and tasks that must be implemented for the efficient implementation of data protection safeguards set out under Ley Orgánica 3/2018¹⁵⁰⁰ and the GDPR.¹⁵⁰¹

Correspondingly, we also observed that in addition to these regulations in terms of data protection, the Order stipulated that the parties must ensure compliance with Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration, which we believe that extend the scope of vast number of responsibilities attributed to SGAD, which was merely attributed to Telefonica company for Covid Asistencia application. Although, till date, there were not any repercussions observed regarding this approach implemented in Resolution of October 13, 2020, from data protection law perspective, it still seems safer option to delegate most of the important accountabilities to the private third-party

¹⁴⁹⁹ Article 2 of «BOE» núm. 273, de 15 de octubre de 2020, pp.8839188398, “Obligaciones de las partes con relación a la delegación de competencias prevista en la letra a) de la cláusula primera:” <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-12339>.

¹⁵⁰⁰ Article 32 of the GDPR, security of processing.

¹⁵⁰¹ Article 32 of Ley Orgánica 3/2018, seguridad del tratamiento.

companies with strict oversight mechanism owned by the relevant public authorities to prevent any negligence pertaining to the safeguards stipulated within the scope of the Order. That being said, this is only relevant to the administrative and regulatory aspects of the Order and resolutions. We will still deep dive into the technicalities and data protection law aspects of both applications in Chapter 7 in detail, as we only discussed those from regulatory perspective.

Lastly, we believe that as efficient mechanism for the efficient and consistent implementation of the agreement between parties for the application, both parties to the resolution accepted to keep each other informed about any incident or relevant fact of which they are aware that may affect the operation of the Application, periodically exchanging updated data on its use and management to monitor its effectiveness and the management of the pandemic.¹⁵⁰² Furthermore, they agreed to keep each other informed of any relevant incident or fact of which they are aware that may affect the operation of the application. To this end, updated data was promised to be provided periodically on the use and management of the application as well as monitoring its effectiveness in managing the pandemic. The signatory parties undertook to resolve by mutual agreement, within a Monitoring Commission, any discrepancies resulting from the interpretation and compliance of this Agreement. Such Monitoring Commission was chaired by the Secretary General of Digital Administration or an official whom he delegates, made up of six members, three belonging to the SGAD and three belonging to the Ministry of Health.¹⁵⁰³

From our angle, it is positive enough, the similar approach was also taken by the Resolution of 30 April, for Covid Asistencia application, namely establishing a similar type of monitoring committee for the efficient

¹⁵⁰² Article 7 of BOE núm. 273, de 15 de octubre de 2020, pp.88391-88398, “Comisión de Seguimiento, Deber de Información Mutuo Y Resolución de Controversias”.

¹⁵⁰³ Article 7 of BOE núm. 273, de 15 de octubre de 2020, pp.88391-88398, “Comisión de Seguimiento, Deber de Información Mutuo Y Resolución de Controversias”.

implementation of the agreement, which composed of the Secretary-General for Digital Administration, who shall preside over it, a Member with the rank of Deputy Director-General, who shall serve in the Secretary-General for Digital Administration, appointed by the Secretary-General for Digital Administration, and two Members appointed by Telefónica.¹⁵⁰⁴ Therefore, in light of this diligent approach for both technical and organizational measures set out above and efficient and healthy implementation of the contractual requirements for both of applications, i.e., Radar Covid and Covid Asistencia, we are of the view that within such a short notice to establish a legal and contractual framework, the Ministry of Health, SGAD and other authorities that were involved in these processes did relatively a good job. To put differently, even though we are also aware of the fact that these arrangements are not telling plenty of details by itself, in isolation with the other legal framework established by the Government, it is still a positive step towards to exercising due care about the right to privacy of data subjects in society using these applications. Moreover, regardless of the applications itself, these resolutions also played a significant role in organizing the coordination between the public authorities and developer third-party companies. The same could be easily provided for the Order itself, as it introduced the idea of the specific symptom checking application and data collection for statistical purpose to get more visibility of Covid-19, which we believe at the same time paved the way for more extensive and detailed application for contact tracing activities, namely Radar Covid, whose details will be discussed within Chapter 7, as mentioned.

That being said, we, still, do not simply conclude that such resolutions decrees are error-free and satisfied each and every legal requirement perfectly for both data protection law and wider legal issues arose as part of pandemic, but rather, they were at least created with the intent of tackling the ambiguity and assisting the Covid as articulated by them, which we find diligent. In other words, evidently, these resolutions are still promising tools for regulators to

¹⁵⁰⁴ Article 13 of BOE núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829, “Comisión de Seguimiento”, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4829.

increase level of transparency by making these agreements publicly available and delineating strict rules on the implementation of data subject rights as well as deletion of personal data attributed to the sub-processor and processor. It still does not fully exclude the previously mentioned feared events associated with the applications in terms of governments' increased surveillance capabilities, yet at least it might be useful to tackle concerns related to negligence of data protection rights during such emergency situation, and abuse of access to personal data of users by third party sub processor technology companies going forward, in case applications become operationalized in the future. Nevertheless, as briefly mentioned herein and will be detailed in Chapter 7, lack of clarity on the responsibility and accountability of controller and processors is concerning. Suitably, we are of the view that going forward, the best way would handle such ambiguity with a devoted regulation as indicated in previous section, rather than restrictive orders and decrees for general management of pandemic scenarios, not only privacy matters. By doing this, the necessity of providing more tailored made approach to pandemics and establishing more detailed framework on each institution would be tackled by the regulators.

4. Implementation of Data Protection Law Necessities in Spain during the pandemic

With regards to the general outlook of data protection and privacy matters in Spain throughout the pandemic, on the one hand, existence of the GDPR¹⁵⁰⁵ and Ley Orgánica 3/2018¹⁵⁰⁶ are already covering such extraordinary cases as part of the listed lawful basis of processing activities, on the other hand, there is an ambiguity resulted from the interpretation of the situation, namely dilemma of protecting right to data protection versus right to life, which has been discussed across the previous chapters from the European Law

¹⁵⁰⁵ See Article 2-I of the GDPR: defines the territorial scope of the regulation. It specifies that the GDPR applies to the processing of personal data of data subjects who are in the European Union (EU) by a controller or processor, regardless of whether the processing occurs in the EU or not, as long as the processing activities are related to offering goods or services to those data subjects in the EU or monitoring their behavior within the EU.

¹⁵⁰⁶ See Article 5 of Ley Orgánica 3/2018, already mentioned.

perspective. However, from our perspective, to strike the balance of both in Spain, as briefly touched in previous sections, while we should not ignore the our rights, more specifically, in line with our remit, right to data protection, such constant chase of the “normal” should also be implemented in terms of healthcare, which is a similar approach to what we have provided for Decreto de Alarma in this chapter. To this end, On March 13, 2020, the Spanish Data Protection Agency (“AEPD”) released a report¹⁵⁰⁷ scrutinizing the handling of personal data concerning the circumstances arising from the spread of the COVID-19 virus.¹⁵⁰⁸ The AEPD emphasized that, in general, regulations pertaining to the protection of personal data, aimed at upholding fundamental rights, are fully applicable in the context of the pandemic. This is because there is no rationale for the suspension of fundamental rights, nor has any such measure been enacted. Nonetheless, the personal data protection legislation itself incorporates the necessary safeguards and regulations to legitimately permit the processing of personal data in situations, such as the current health emergency of widespread impact.¹⁵⁰⁹ As a result, the AEPD emphasized that the handling of personal data in the present health emergency must align with the aforementioned personal data protection regulations. Hence, all the principles outlined in Article 5 of the GDPR and Ley Orgánica 3/2018 must continue to be adhered to in the course of processing activities.¹⁵¹⁰ As such, we are of the view that such approach is also compatible with what Mr. Jean-Philippe Walter, Council of Europe Data Protection Commissioner, provided by putting forward that although these restrictions are appropriate and comprehensible, they should, however, be

¹⁵⁰⁷ For the full report see AEPD, (2020) “Report From The State Legal Service (Detached Department of the SIs at the Spanish DPA) On Processing Activities Relating To The Obligation For Controllers From Private Companies And Public Administrations To Report On Workers Suffering From Covid-19” available at: <https://www.aepd.es/documento/2020-0017-en.pdf> (accessed on 23 June 2024).

¹⁵⁰⁸ EU Agency For Fundamental Rights, (2020) “Coronavirus COVID-19 outbreak in the EU Fundamental Rights Implications (Spain)” available at: https://fra.europa.eu/sites/default/files/fra_uploads/spain-report-covid-19-april-2020_en.pdf (accessed on 16 October 2023), p.8.

¹⁵⁰⁹ *Ibid.*

¹⁵¹⁰ AEPD, (2020) “Report From The State Legal Service.....”, *op.cit.*, p.5.

valid, extraordinary, and time-limited in nature.¹⁵¹¹ The fundamental principles of Convention 108 must be upheld, and data subject rights must be safeguarded, if they include processing personal data,¹⁵¹² the similar logic provided by AEPD for the clear implementation of Ley Orgánica 3/2018 provisions, as we also delineated in the previous section of this chapter for the need of a new legal regulation specific to pandemics.

That being said, it was evident from the beginning of the pandemic that the situation was not that simple, particularly considering the complexity of legal regime that applies to pandemic scenarios in Spain as elaborated and analyzed above. Likewise, there are also challenges on data protection perspective, which resulted from the nuances of Ley Orgánica 3/2018, because in addition to adapting the Spanish legal system on data protection to the GDPR, the Spanish Data Protection Law, i.e., Ley Orgánica 3/2018 includes an additional Chapter - Articles 79 to 97- on guaranteeing the digital rights of citizens and employees beyond the GDPR,¹⁵¹³ which will impact on the lawful basis discussion in the following section as well. For example, among other differences, the most remarkable difference is that transparency and information. In addition, the chapter on digital rights, extending beyond the GDPR, encompasses various aspects. These include provisions concerning internet neutrality, ensuring universal internet access, enhancing digital security, promoting digital education, safeguarding privacy related to the usage of digital devices within workplaces, guaranteeing the right to disconnect digitally outside of work hours, protecting privacy from video surveillance and sound recording in workplaces, ensuring privacy rights against the use of geolocation systems in workplaces, and establishing the

¹⁵¹¹ Council of Europe, Covid-19 Data Protection <https://www.coe.int/en/web/data-protection/covid-19-data-protection> (accessed on 23 June 2024).

¹⁵¹² *Ibíd.*

¹⁵¹³ Recio, Miguel; Albiñana, CMS; and Suárez de Lezo (European Audiovisual Observatory) (2019) "Spain Goes Further Than The GDPR When Adapting Its Data Protection Law", *IRIS Legal Observations of the European Audiovisual Observatory*, available at <https://merlin.obs.coe.int/article/8502> (accessed on 15 July 2024), p.2.

right to a digital testament¹⁵¹⁴, which might require further action from data controllers and other public authorities as part of data protection compliance activities during the Covid, into which we will deep dive from this perspective as well. As seen, there are further requirements to be implemented by public authorities in terms of further details to be provided to data subjects, and further consideration to be paid when any type of surveillance activities at stake.

Correspondingly, the reason why we delineated those differences is that the nuances of Ley Orgánica 3/2018, alongside with characteristics of Spanish legal system makes some parts more challenging for data controllers. For instance, as discussed above, the questions of what absolute right is and what is the definition of suspension must be addressed by the decision makers to envisage any safeguard for right to privacy during pandemic scenarios as briefly called out above. As seen from the differences of Ley Orgánica 3/2018, it is clearly seen from Spanish regulator that rights of data subjects are being treated with utmost care. To give more specific example, given the more restrictive approach on the right of privacy against the use of geolocation systems in the workplace and the right to a digital testament and etc. brought by Ley Orgánica 3/2018, the approach brought by Spanish regulator seems to be more strict compared to the GDPR, and the boundaries of fundamentalism of such right can be interpreted way more widely and in a privacy-friendly manner.

Furthermore, to solidify such approach on fundamentalism of data protection or right to privacy, we believe that what a Spanish constitutional perspective brought thereon is also crucial to understand the nature of the right in Spain. As per the Constitution, more specifically Article 55.1, right to privacy is a right that, not similar to others, cannot be suspended, even if any type of emergency state is declared.¹⁵¹⁵ Similarly, Article 18.4 of the Spanish

¹⁵¹⁴ Recio, Miguel; Albiñana, CMS; and Suárez de Lezo, European Audiovisual Observatory (2019) "Spain Goes Further ...", *op.cit.*, p.2.

¹⁵¹⁵ García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain..." *op.cit.* para 10.

Constitution recognizes the fundamental right to the protection of personal data.¹⁵¹⁶ The rights provided in the article are of a very personal and independent nature, in such a way that the exercise of one is not a requirement for the exercise of the other, being regulated in Organic Law 7/2021, of May 26, on data protection.¹⁵¹⁷ Likewise, from data protection perspective, also AEPD, through its another report published, is of the view that the fundamental right to the protection of personal data cannot be suspended due to this emergency,¹⁵¹⁸ which we find critical to evaluate the nature of the right and urge authorities to act accordingly.

Therefore, considering these, our evaluation on the topic is that existence of such alarming regulations would mean to the limitation of certain rights, including but not limited to right of privacy to some extent, due to the compelling reasons as detailed in the order, and elaborated above. To this end, we also partially agree with the perspective brought by Rodríguez Ayuso, as throughout this study¹⁵¹⁹, they have concluded that the declaration of a state of alarm due to the health crisis stemming from COVID-19 did not directly or indirectly imply the suspension of the fundamental right to data

¹⁵¹⁶ Article 18 of the Spanish Constitution:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

¹⁵¹⁷ Gobierno De España, Ministerio Del Interior, (2023) "Right of Access to the File "PERPOL" https://sede.policia.gob.es/portalCiudadano/en/tramites_ciudadania_antecedentespoliciales_derechoacceso.php# (accessed on 3 September 2023)..

¹⁵¹⁸ AEPD (2020) Notice on Corona Virus Self-Assessment Apps and Websites <https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites> (accessed on 23 June 2024).

¹⁵¹⁹ For the full study see Rodríguez Ayuso, Juan Francisco (2020) "Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia", *Revista de bioética y Derecho*, vol.50, pp.353-368.

protection, although it did lead to the implementation of certain actions that could limit it.¹⁵²⁰ From our perspective, such limitation, particularly indirect ones, are somehow inevitable, given the nature of the right to data protection and privacy rights, which are strictly intertwined with other parts of fundamental rights as detailed above, particularly adding the geolocation tracking, thereby, indirectly impacting their movements, as another concern as well. However, we believe that such limitation on right of privacy should be at least in line with the most fundamental principles of processing activities delineated under the article 5 of the GDPR, and article 5 of the Ley Orgánica 3/2018. By respecting the most fundamental values attributed to the processing activities¹⁵²¹, it is still possible to implement some extent of protection of privacy while implementing the other grounds. Such approach was also defended by the study of Quiroga Sánchez del Campo, which dealt with right to personal data protection during health emergencies. Quiroga Sánchez del Campo's study provided that they believe it is necessary to take into account the special circumstances involved and the seriousness of the situation, thus applying the principle of proportionality (without implying freedom and complete absence of requirements).¹⁵²² Their conclusion is that while the essence of the right has not been violated, in some cases, the admissible limit was reached due to the unclear adequacy of the proposed controls and guarantees, with insufficient transparency.¹⁵²³

To this end, we are of the view that what Decreto de Alarma provided for the other fundamental rights could be leveraged to right to privacy in general sense for any limitation imposed during pandemics. To elaborate this on, as provided by the extension of the State of Alarm that as has been indicated in the previous royal decrees of extension, constitutional jurisprudence requires

¹⁵²⁰ Rodríguez Ayuso, Juan Francisco (2020) "Control de la privacidad por parte...", *op.cit.*, p.367.

¹⁵²¹ See Article 5 of the GDPR, principles.

¹⁵²² For the full study see Quiroga Sánchez del Campo, María. (2022) "El derecho a la protección de datos personales frente a emergencias sanitarias" Universidad Pontificia Comillas, Facultad de Derecho, pp. 1-46.

¹⁵²³ Quiroga Sánchez del Campo, María (2022) "El derecho a la protección ...", *op.cit.*, p.46.

developing such an analysis taking into account the identification of the intended constitutionally legitimate purpose and compliance with the requirements of the proportionality judgment through compliance with the triple condition of adequacy, necessity and proportionality in the strict sense (among others, SSTC 64/2019, of May 9, FJ 5; 99/2019, of July 18, FJ 6), as elaborated and addressed above.¹⁵²⁴ Therefore, in line with our view, and as supported by the AEPD, while health data may be processed during emergency situations to prevent the spread of the disease causing the health crisis, the processing of personal data must be restricted to what is necessary for its intended purpose, which is because the fundamental right to data privacy protection remains applicable.¹⁵²⁵

On the top of that, with regards to the necessity of such limitation on right to privacy, as delineated by the report of the Library of Congress, in order to effectively guarantee the common interest, the authorities must ensure the legitimate use of personal data that is compatible with those measures.¹⁵²⁶ The AEPD aided health authorities in achieving this by giving them criteria that make these objectives compatible.¹⁵²⁷ Hence, as seen, personal data related limitations must serve very important target for the healthcare of the public, and must serve to a legitimate purpose. Regarding such legitimate purpose, according to what was expressed by the Constitutional Court in its Order of April 30, 2020 (FJ 4), the objective of the measures contained in this extension finds "[...] enough constitutional coverage in the articles 15 CE (guarantee of the physical integrity of people) and 43 CE (protection of health), both so intensely connected that it is difficult to imagine them separately,

¹⁵²⁴ See Section 2 of Real Decreto 555/2020, de 5 de junio, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. <https://www.boe.es/buscar/act.php?id=BOE-A-2020-5767#a1>.

¹⁵²⁵ AEPD (2020) Informe 017/2020 on the Treatment of Data Derived from the Present COVID-19 Virus Situation (Mar. 12, 2020), <https://perma.cc/Z8GA-655Y>. (accessed on 23 June 2024).

¹⁵²⁶ The Law Library of Congress, Global Legal Research Directorate (2020) "Regulating Electronic Means to Fight...", op.cit., p.152.

¹⁵²⁷ The Law Library of Congress, Global Legal Research Directorate (2020) "Regulating Electronic Means to Fight...", op.cit., p.152.

especially in the current circumstances", since they are "[...] limit the impact that the spread of COVID-19 may have on the health of human beings, on their physical integrity and on their right to life.¹⁵²⁸ Consequently, our evaluation on this approach is that it might create a legal ground for the implementation of privacy-restraining acts as well, in particular during the management of pandemic scenarios. Particularly, we also believe that such approach would oblige national authorities to act in line with the adequacy, necessity and proportionality which is also reiterated by the EDPB and AEPD several times with regards to the processing activities, as also detailed in previous chapters, as the natural outcome of these compatibility and limited use of the restrictions thereon. Within the similar vein, we believe that the perspective brought by Valero Torrijos, and Cerdá Meseguer is also in line with this view, which we find supportive of our general approach through this chapter.¹⁵²⁹ In more detail, they provided that the concern for the protection of personal data must undoubtedly be a priority when facing this challenge, especially in the context of public health. However, the key questions to ask are not so much what measures can be adopted, for what purposes data can be used, or who can process them, but rather how to do it. This requires adopting an alternative approach to the one traditionally maintained in this field, integrating data protection requirements, and considering other perspectives and dimensions. Their proposed integration allows for the exploitation of the undeniable added value that technological innovation can provide, with appropriate legal guarantees.¹⁵³⁰

¹⁵²⁸ See Section 2 of Real Decreto 555/2020, de 5 de junio, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. <https://www.boe.es/buscar/act.php?id=BOE-A-2020-5767#a1>.

¹⁵²⁹ For the full study see Julián Valero Torrijos and Juan Ignacio Cerdá Meseguer. (2020) "Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del COVID-19", *EUNOMÍA, Revista en Cultura de la Legalidad*, vol.19, pp. 103-126.

¹⁵³⁰ Torrijos, Julián Valero, and Juan Ignacio Cerdá Meseguer (2020) "Transparencia, acceso y reutilización de la información ...", *op.cit.*, p.125.

Therefore, as we supported through the entire research that in addition to the lawfulness of processing activities implemented in Spain during the pandemic, we would also like to enlighten a topic with regards to the exercise of data subject rights from the data protection perspective, during the state of the alarm, which creates one of the most heated part of data subjects' protection. The reason behind such discussion is, as known, access to justice has also been significantly impacted by the restrictions on freedom of movement established by Decreto de Alarma 463/2020, particularly because its second additional provision specifies the suspension of process deadlines in the following terms.¹⁵³¹ For all jurisdictional orders, terms are suspended, and time restrictions stipulated in procedural statutes are suspended and interrupted. When this Royal Decree, or any extensions thereof, ceases to be effective, the computation of time restrictions shall be restarted. In the criminal jurisdiction, suspension and interruption do not apply to habeas corpus proceedings, proceedings handled by guard services, proceedings involving detainees, protection orders, urgent prison surveillance proceedings, and any preventative measures involving violence against women or children.¹⁵³²

Similarly, for these circumstances, the courts must re-schedule the hearings in such circumstances. As such, when the Royal Decree loses validity (after 15 calendar days or, where appropriate, when the extension(s) expire) specified interruption would automatically be without effect and will resume as soon as the suspension is lifted due to the disappearance of the state of alarm.¹⁵³³ Nonetheless, there was not any specifics provided on the exercise of data subject rights and the timelines such requests are subject to. For instance, as per the GDPR, these requests must be responded within 30 days.¹⁵³⁴ As such, given the suspension on the jurisdictional timelines during

¹⁵³¹ EU Agency for Fundamental Rights Report, (2020) "Coronavirus pandemic...", *op.cit.*, p.3.

¹⁵³² EU Agency for Fundamental Rights Report, (2020) "Coronavirus pandemic...", *op.cit.*, p.3.

¹⁵³³ For the details of the suspensions, see Decreto de Alarma 463/2020, de 14 de marzo, disposición adicional segunda. Suspensión de plazos procesales.

¹⁵³⁴ EDPB Guideline, (2023) Respect Individuals Rights https://edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en (accessed on 16 October 2023).

the state of alarm, it would also be privacy-friendly approach to set out the fate of data subject access requests that could be raised by data subjects with regards to their health data processed. Particularly, there could be specific measures on special categories of personal data, and thereby, health data of data subjects, even if not entire data categories. Such approach would solidify the data subjects trust against the use of any measures requiring processing of sensitive data as well. Moreover, our approach would also be compatible what Domínguez Álvarez suggested for close relationship between the success of pandemic safeguards and right to privacy.¹⁵³⁵ To provide more detail thereon, they provided that fundamental privacy rights constitute the very foundation of the set of constitutionally recognized rights in the face of the growing processes of digitalization and datafication of society.¹⁵³⁶ Therefore, it is not true that the protection of personal data and its powerful regulation led by the GDPR appear as obstructionist elements, hindering the implementation and realization of necessary personal data processing measures against COVID-19. On the contrary, what is sought, is the correct application of an advanced regulation of a fundamental right, data protection, given that ensuring certain public health guarantees is impossible without safeguarding high standards of personal data protection, which constitutes the basic institute for the full effectiveness and guarantee of the set of constitutionally recognized fundamental rights, standing as the cornerstone of the social and democratic Rule of Law in the face of the digital evolution. Suitably, what we suggested, namely bolstering the data subject rights, would align with the ultimate importance of constitutional protection of right to data protection.

In light of these, on the positive side, AEPD undertook quite proactive approach since the beginning of the pandemic, which is in line with the view of Martínez Martínez provided in their study, as mentioned in their study that

¹⁵³⁵ For the full study see Domínguez Álvarez, José Luis (2020) " Privacidad y salud pública. Una simbiosis compleja pero necesaria para hacer frente a la covid-19". AIS: Ars Iuris Salmanticensis, vol.8, n.2, Recuperado a partir de. pp.200–206. <https://revistas.usal.es/cuatro/index.php/ais/article/view/25699>.

¹⁵³⁶ Domínguez Álvarez, José Luis (2020) "Privacidad y salud pública... ", *op.cit.*, p.206.

the role of these authorities is crucial and essential for the evolution of the fundamental right to data protection, since the Agency is empowered to issue specific instructions, where necessary, to ensure that data processing aligns with the principles of the law.¹⁵³⁷ Alongside these responsibilities, these authorities possess inspection and sanctioning powers, which, given the significance of the enforcement regime in Spain, lend considerable weight to their decisions.¹⁵³⁸ Suitably, similar to this perspective, AEPD took active role in the guidance and enforcement part, latter will be detailed in the next chapter, and reiterated that the fundamental right to the protection of personal data, thereby data subject rights, should not be suspended due to the present emergency circumstances.¹⁵³⁹ Likewise, the AEPD also expressed its concern about this type of action, considering that it involves a particularly intense interference in the rights of the affected parties and that it is being carried out without the prior criterion of the health authorities. This concern relates to the measurement of temperature by businesses, work centers, and other establishments.¹⁵⁴⁰

Subsequently, within the same vein of data subject rights, it is also important to understand the challenge around the exercise of data subject rights. For instance, the involvement of numerous entities in the development and administration of the Radar Covid complicated the exercise of rights granted to individuals under the GDPR. For instance, an individual seeking to safeguard their right of access to personal data processed by the entity responsible for the application may find the institutional complexity discouraging and, as a result, undermine the protection afforded by the

¹⁵³⁷ Martínez Martínez, Ricard (2007) "El derecho fundamental a la protección de datos: perspectivas", *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, vol. 5, 4, pp.1-15, p.15.

¹⁵³⁸ *Ibid.*, p.15.

¹⁵³⁹ EU Agency for Fundamental Rights Report, (2020) "Coronavirus pandemic...", op.cit., p.3.

¹⁵⁴⁰ EU Agency for Fundamental Rights Report, (2020) "Coronavirus pandemic...", op.cit., p.3.

GDPR.¹⁵⁴¹ Although Article 12.3 of Ley Orgánica 3/2018 allows the processor to handle, on behalf of the controller, the requests for the exercise of rights made by data subjects, this is a voluntary arrangement. Therefore, the processor responds to the data subjects if it is stipulated in the contract or legal agreement that binds them to the data controller. The alterations in the administrative structure of the Ministry of Health that occurred during the pandemic, especially during the development phase of the positive case tracking application, did not enhance the position of users and other concerned parties whose personal data could be impacted. On the top of these, the challenges in the external dimension are compounded by issues of transparency, frequent modifications in various accompanying documents related to the application, and the emergence of numerous press reports highlighting security breaches and risks to the protection of personal data.¹⁵⁴² We, hence, believe that the most optimal solution for mitigating this particular problem is to solidify the level of transparency on both processing activities and content and limits of data subject rights, as detailed in the next section for the information requirement of Radar Covid application as well, not to expose any type of uncertainties on personal data of people in Spain.¹⁵⁴³ In this regards, we agree with the approach brought by Márquez Carrasco and Ortega Ramírez¹⁵⁴⁴ which provided that undoubtedly, during times like the pandemic, digital monitoring methods are beneficial tools. However, they also serve as a means of regulation that, especially in a health crisis, should be

¹⁵⁴¹ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» and protection of personal data. An analysis of the disciplinary procedures of the Spanish Data Protection Agency", *InDret*, vol.4, pp. 249-280, p.272.

¹⁵⁴² Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» and protection of personal data. ...", op.cit., p.272.

¹⁵⁴³ For the full Guidance see ECHR Guide on Article 8 of the European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/guide_art_8_eng (accessed on 3 October 2023).

¹⁵⁴⁴ Márquez Carrasco, Carmen and Ortega Ramírez, Juan Antonio (2020) "COVID-19 and the Challenges of Digital Surveillance for Human Rights: Analysis of the App DataCOVID Foreseen in the Ministerial Order SND/29/2020, of March 27th", *Rev. Bioética & Derecho*, vol. 50, pp.205-220, p. 205.

governed by information, transparency, public responsibility, and legal oversight.¹⁵⁴⁵

The essential underlying reason of our proposal is that like the complexity of identification of the relevant body or person in charge with implementation of data subject requests, there are certain criticisms directed towards legal basis of processing activities and providing relevant information to the data subjects are of quite visible. The second one will be discussed in the next section as said, but for the implementation of data subject rights, we are of the view that during pandemic the most fundamental challenge is to understand the scope of these rights set out under both GDPR and Ley Orgánica 3/2018, and perceive whether they are still applicable to data subjects without any hinderance or alteration, due to the alarming nature of pandemics. Therefore, our assessment on the topic is that data controllers must precisely analyze and understand the legal restraints resulted from above mentioned Orders and Decrees, and provide the most accurate and digestible interpretation of these restraints on users' rights in a manner that was asked by EDPB¹⁵⁴⁶ and AEPD.¹⁵⁴⁷ By this method, we believe that, both challenge of interpretation of the limits of data protection rights as well as the intrusiveness of processing activities could be easily understood by data subject users, given that pandemic and data protection has been relatively new and unique combination due to their nature in our era, and that there are plenty of theoretical assumptions based on the interpretation of our daily lives.

Furthermore, from our perspective, it is important to deep dive on the Decree to analyze whether there might be any indirect data protection implications resulted therefrom, to interpret data protection as a whole during pandemic scenarios. As detailed in first section of this Chapter, for some scholars and legal practitioners, the Decree exceeds the scope that the Constitution and

¹⁵⁴⁵ Márquez Carrasco, Carmen and Ortega Ramírez, Juan Antonio (2020) "COVID-19 and the Challenges of Digital Surveillance....", op. cit., p. 205.

¹⁵⁴⁶ See EDPB Guidelines (2020) 05/2020 on consent under Regulation 2016/679, p.15.

¹⁵⁴⁷ See AEPD Guidelines, (2019) "The Duty To Inform And Other Accountability Measures For Mobile Devices", available at: <https://www.aepd.es/documento/nota-tecnica-apps-moviles-en.pdf>, p.1.

Organic Law 4/1981 recognize the state of alarm, being unconstitutional.¹⁵⁴⁸ Similarly, there were plenty of discussions around the misinterpretation of the term of limitation and restriction as well, as discussed in detail. For instance, as provided in the referred article that In the state of alarm, it is only possible to limit rights; in exception (and place), it is possible to suspend them.¹⁵⁴⁹ Thus, understood, the state of alarm implies the adoption of measures that may entail limitations or restrictions on the exercise of fundamental rights, that is, all these rights remain in force.¹⁵⁵⁰ However, from data protection perspective, our evaluation is of two-fold approach. Firstly, the declaration of the state of alarm neither suspended the effectiveness of the GDPR, nor emptied of content the fundamental rights to privacy and personal data.¹⁵⁵¹ In other words, although this is certainly an important topic, it does not necessarily within the scope of our study.

Having said that, we must admit that all this criticism might also provide an important standpoint for the implementation of data protection and privacy rights of individuals in society. Reliance on such discussion point automatically leads us to the long-standing discussion of fundamentality of privacy right of the individual, as briefly discussed in the second section of this chapter as well, which was briefly touched above for the need of a new legal regulation. Nevertheless, despite the ongoing discussions around this notion, our evaluation on the topic is that the approach of the EU to the topic is crystal clear and based on the Charter of Fundamental Rights of the European Union stipulates the protection of personal data¹⁵⁵², it is no doubt that right to privacy

¹⁵⁴⁸ For the full details of this approach see Méndez-Monasterio Silvela, Pablo (2021) “Sobre la inconstitucionalidad del Real Decreto 463/2020 por el que se declara el Estado de alarma”, Conflegal, <https://conflegal.com/20210723-opinion-sobre-la-inconstitucionalidad-del-real-decreto-463-2020-por-el-que-se-declara-el-estado-de-alarma/> (accessed on 22 June 2024).

¹⁵⁴⁹ Tirant (2021) “El TC estima parcialmente el recurso contra preceptos del Real Decreto 463/2020, que declaró el estado de alarma para la gestión del Covid-19” <https://tirant.com/actualidad-juridica/noticia-sentencia-estado-de-alarma/> (accessed on 22 June 2024).

¹⁵⁵⁰ *Ibíd.*

¹⁵⁵¹ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) “Radar COVID» and protection of personal data...”, *op.cit.*, p.272.

¹⁵⁵² Article 8 of the Charter of Fundamental Rights of the European Union <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

is a fundamental right and it falls within the scope of any sort of limitations resulting from any type of Decree that aim to limit certain rights during extraordinary situations, as also delineated above by using AEPD and Constitutional Court decisions. Similar approach also provided by the study of Andreu Martínez. The study provided that, a fundamental issue to address is determining adequate safeguards for protecting citizens' fundamental right to data protection and norms where these measures are established, in connection with legal reservation (Art. 53.1 CE) and the relatively stringent doctrine of the Constitutional Court on this matter (Judgments 292/2000; 76/2019, the latter referring to especially protected data).¹⁵⁵³ Hence, as seen, Andreu Martínez indicated the reason of its fundamentalism by building on Constitution and the Constitutional Court decision, which we also think it should simply supersede all the ambiguity, give a rise to the importance of safeguards to be implemented by authorities.

Nonetheless, we also believe the reason why such ambiguity arose regarding the fundamentality of right to privacy is that the European Convention on Human Rights in Article 8.2 clearly articulates that interference with a person's private life can only occur "insofar as it is provided for by law and constitutes a necessary measure in a democratic society for national security, public safety, the economic well-being of the country, the defense of order and the prevention of crime, the protection of morals or health, or the safeguarding the rights and freedoms of others."¹⁵⁵⁴ In case we deep dive into the interpretation of this as per the Guidance ECHR¹⁵⁵⁵, while it is evidently presenting right to data privacy as one of the fundamental human rights, it is, at the same time, opening doors for interference of a door for extreme cases listed, which we believe might create a valid excuse for halting right to privacy during extreme cases. Within the similar context, for example, we should

¹⁵⁵³ Andreu Martínez, Belén (2020) "Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19", *Actualidad Jurídica Iberoamericana*, n.12 bis, pp. 848-859, p.858.

¹⁵⁵⁴ Article 8.2. of the European Convention on Human Rights <https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0>.

¹⁵⁵⁵ For the full Guidance see ECHR Guide on Article 8 of the European Convention on Human Rights.

recall that the historical jurisprudence of Spanish Constitutional Court and generally from any European Constitutional body, rights are not absolute and, in case of conflicts, they can be reduced to their essence to preserve the exercise of other superior or preponderant rights.¹⁵⁵⁶ In the same direction, we are of view that it is necessary to ask the following question: How powerful or prioritized should this right to privacy be, and to what extent can it be limited in favor of public health?

In our opinion, from data protection point of view, although there are not many implications resulted from the Decrete do Alarma, contrary to the above discussion points, there still might be new type of discussions related to legality of limitation of data protection right, as it is also considered as one of the most important rights, an as discussed above, it should be included in the new legislation specific to the pandemics. To provide more specific detail, even though there should be a balance to be stroke between public interest and personal interest from the legal perspective as discussed across the previous Chapters for the other European jurisdictions, employing the limited and proportionate restrictive measures could be preferred rather than the entire limitation of the right at stake. Thus, as mentioned above, at least adhering to the most fundamental data protection principles, such as the legality of processing, purpose limitation, data minimization and others set out under article 5 of the GDPR would minimize the impact and help regulators to strike a balance between both aim and such approach would not prevent decision makers from their duties to safeguard the public health. To put it differently, it is understandable that from the regulator perspective, when there is a Decree at stake, it is not always easy to talk about privacy-by-design or employing most cutting-edge technologies to prevent profiling of data subject. Hence, given the urgent nature of the situation and the regulatory act, reiterating the importance of complying with the measures would be sufficient to some extent. Having said that, we would like to state that we find the conclusion of Rivas Castillo's study in line with agree with the perspective

¹⁵⁵⁶ European Commission For Democracy Through Law (Venice Commission), Judgment Of The Constitutional Court Of Spain Of 19 November 2020, p.8.

brought by ourselves. In more detail, we also agree with the conclusion of Rivas Castillo on surrounding data protection, namely it is apparent that data protection surrounding seems to be up-to-date and applicable at both the European and national levels.¹⁵⁵⁷ However, in line with our recommendations above, such positive outlook should be bolstered with a balanced approach we proposed between health and privacy necessities, as well as efficient safeguards to be deployed. On the positive side, there are not many major data breaches nor complaints raised to AEPD pertaining to the implementation of these safeguards. Rather there is a few relatively minor issues predominantly resulted from digital contact tracing activities, which will be detailed in the last chapter.

Consequently, in summary, the effectiveness of actions taken by competent authorities, particularly health authorities, in the fight against the epidemic cannot be hindered or limited by data protection legislation because it offers solutions that allow for the lawful use of personal data to be in line with the actions required to guarantee the common good on effective basis, similar to the discussions above. However, at the same time, it is positive to observe that, AEPD took a proactive role by publishing its pro-privacy reports during the entire pandemic, which definitely solidified the significance of GDPR and Ley Orgánica 3/2018 for controllers and shed light onto the obstruction generated by the pandemic due to its unique nature. Such guidance must have also helped authorities to react as quick as possible and bolster the requirements of fundamental requirements of data protection law necessities, considering that they acted quickly in relation to the concerns raised by individuals and scholars, as detailed in next sub-chapter and Chapter 7. Hence, it is significant to remind that a health emergency does not generate a kind of legal sandbox, which allows public decision-makers a wide margin of maneuver to design tools without assuming any type of legal

¹⁵⁵⁷ David Rivas, Castillo (2020) "Protección De Datos: Evolución, Actualidad, Análisis Y La Influencia Del Covid-19" , Universidad de Jaén, <https://hdl.handle.net/10953.1/12895>, pp.1-38, p.34.

responsibility.¹⁵⁵⁸ Hence, right to data protection should be included in the limitation of fundamental rights discussions in case any pandemic arises again in the future.

5. Lawful Basis of Data Processing Activities by the Applications

As detailed in previous Chapters, during the COVID-19 pandemic, various countries, including Spain, implemented measures and guidelines to facilitate contact tracing efforts through digital applications. As an also well-known matter that, the digital contact tracing measures in Spain also aimed to control the spread of the virus while respecting data protection and privacy rights. Particularly, as a legal foundation of the applications, following actors involved in the process. These are namely, the GDPR, and LOPDyGDD¹⁵⁵⁹, which complements and supplements the GDPR at the national level and provides additional guidelines for data protection, including the processing of health data.

Furthermore, the guidelines of AEPD¹⁵⁶⁰ undertook a significant role in assisting data controllers for ensuring their compliance with data protection regulations in Spain. To this end, due to COVID-19 limits, Spain's data protection agency, AEPD, published multiple guidelines with respect to utilizing mobile applications to access and monitor the capacity of public venues, which will be more detailed in Chapter 7. In other words, to simply indicate the process in Spain, AEPD seemed to undertake a crucial role in the design and usage of applications to restrict access to public spaces and social distance as well, in addition to the existing regulations, as itself also indicated

¹⁵⁵⁸ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» and protection of personal data. ...", *op.cit.*, p.272.

¹⁵⁵⁹ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

¹⁵⁶⁰ AEPD is an independent public authority in charge of ensuring the privacy and data protection of citizens, as detailed in their main website <https://www.aepd.es/es/la-agencia/bienvenida-la-agencia> (accessed on 2 August 2023).

this in its general statement issued¹⁵⁶¹. Additionally, on 27 March 2020, through the Order SND/297/202, which was elaborated in the previous section of this Chapter, the SEDIA, was requested to create a contact-tracing app to assist the handling of covid pandemic, and requested a data analysis for pandemic purposes accordingly.¹⁵⁶² However, as detailed above, it did only act for a legal basis of establishing symptom checker application (Asistencia Covid) and data analyze program, but it did not have any linkage with Radar Covid app, which is the main discussion point of this section, as national contact tracing application, therefore, we will not touch base the Order again, but rather this section is merely focused on the legal basis of processing activities by the national contact tracing application of Spain, rather than reviewing those various orders in detail. Lastly, Agreement of October 9, 2020, between the Ministry of Economic Affairs and Digital Transformation (Secretariat of State for Digitization and Artificial Intelligence) and the Ministry of Health regarding the Radar Covid application is another source of legal basis, in addition to all these aforementioned sources. As such, it is fair to state that each of above-mentioned regulations and guidelines entail the legal framework for data protection and privacy considerations for the deployment of contact tracing applications in Spain in its entirety. However, we must remind that all of those are of secondary role, as such, the main and most vital lawful basis of the processing activities implemented by the national contact tracing application Radar Covid was brought by the GDPR and Ley Orgánica 3/2018, as also reiterated by the AEPD.

Accordingly, after the general description of the legal landscape of Spanish digital contact tracing activities across the country, we would like to deep dive on the nuances of lawful basis. First, from the perspective of legal basis of the processing activities, to begin with, Spanish controller listed all of these

¹⁵⁶¹ AEPD (2020), Notice on coronavirus self-assessment apps and website <https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites> (accessed on 7 August 2023).

¹⁵⁶² Order SND/297/2020 (27 March 2020).

applicable lawful basis grounds as part of GDPR and Ley Orgánica 3/2018, which are identical for many aspects, as lawful basis of the processing activities. More specifically, as we could see that Radar Covid referred to these following articles of the GDPR 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) and 9.2.i), as for the legal basis of the processing activities. Certainly, this wide range of lawful basis, which is different than the general approach of the data controllers based in other countries detailed in Chapter 1 and 3. To interpret what it means in the real life, we can provide that such wide array of lawful basis for the processing activities open the door for each of the following legal basis; conforming to a legal obligation that applies to the controller, safeguarding the vital interests of the data subject or another individual, and fulfilling a task undertaken for the public interest or as part of the controller's official authority. Having said that, AEPD reiterated the similar criteria for lawful data processing, ¹⁵⁶³ both of which align each other.

Additionally, it also emphasized the use of consent as the legal basis within the scope of article 6-1-a¹⁵⁶⁴ and 9-2-a ¹⁵⁶⁵ of the GDPR, for both personal data and special categories of personal data. As described in Chapter 1 and 3, most of the EU/EEA Member States opted for the combination of consent and legislation as a lawful basis of the processing activities.¹⁵⁶⁶ Therefore, we can safely provide that like many other controllers, Spanish controller did not deviate from the safest path of combining both consent and public health lawful grounds. As also stated by Wairimu and Momen, that such consent-based approach grants users' authority, allowing them to manage their personal data by having the right to retract their consent whenever they wish,

¹⁵⁶³ Vicente Díaz, Matilde and Callejo Carrión, Soraya (2021) "On alarms, geolocations and rights...", *op.cit.*, p.141.

¹⁵⁶⁴ See article 6-1-a of the GDPR, Conditions of processing, consent.

¹⁵⁶⁵ See article 9-2-a of the GDPR, processing of special categories of personal data, consent.

¹⁵⁶⁶ Lintved, Mona Naomi (2021) "COVID-19 Tracing Apps as a Legal Problem: An Investigation of the Norwegian 'Smittestopp' App", *Oslo Law Review*, Vol 8. Issue 2, pp.69-87, p.81.

thereby halting any additional processing.¹⁵⁶⁷ However, this is only the beginning of the discussion. In other words, from our angle, the most remarkable choice of legal basis of the processing activities of Radar Covid is purposes of preventive or occupational medicine within the scope of article 9-2-h¹⁵⁶⁸ of the GDPR and safeguarding the vital interests of the data subject where they are physically or legally incapable of giving consent, as per the article 9-2-c of the GDPR.¹⁵⁶⁹

Respectively, with regards to g), h), and i) of article 9 of the GDPR, these circumstances may be examined jointly, as AEPD indicated, inasmuch as both refer to a public interest, the first of which is described as "essential" and the second of which refers to a public interest described "in the field of public health, such as protection against serious cross-border threats to health," all on the basis of Union law or the law of the Member States laying down appropriate and specific measures to protect the right.¹⁵⁷⁰ The combination of all these measures would permit the processing of personal data when it is necessary for, among other things, determining whether a self-diagnostic test result is positive or negative through telephone assistance or the use of a mobile phone application. It would also permit the transmission of this information to the staff who are in charge of sending recommendations and notifications to the patient and monitoring their progress.¹⁵⁷¹ This approach

¹⁵⁶⁷ Wairimu, Samuel, and Momen, Nurul (2021) "Privacy analysis of Covid-19 contact tracing apps in the EU", *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings, n.25*, pp. 213-228. Springer International Publishing, p.16.

¹⁵⁶⁸ For the full article see 9-2-h of the GDPR, "purpose of preventive or occupational for processing of special categories of personal data".

¹⁵⁶⁹ For the full article see 9-2-c of the GDPR, "vital interest of data subject for processing of special categories of personal data".

¹⁵⁷⁰ Rodríguez Ayuso, Juan Francisco (2020) "Compliance with the regulations on personal data protection in a state of alarm by Public Administrations", Faculty of Law and Administration of the Jagiellonian University, Law Against Pandemic, available at: <https://lawagainstpandemic.uj.edu.pl/2020/05/20/compliance-with-the-regulations-on-personal-data-protection-in-a-state-of-alarm-by-public-administrations/> (accessed on 10 December 2023).

¹⁵⁷¹ *Ibid.*

has not been common in other EEA states, and certainly implementing .1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) and 9.2.i) at the same time must have been a bold decision as it might be open to confusion and ambiguity. Therefore, we are also aware that it is not easy to conclude swiftly by saying that such wide approach in terms of the lawful basis is the best solution for the implementation of legal basis. Obviously, there are plenty of advantages associated with the use of many of these legal bases, to facilitate the use of application, and thereby incentivizing people to use it without any obstacle. From the health efficiency perspective, as discussed in the previous chapters, aiming to remove any obstacle for the processing activities by using wide open set of lawful bases, which could certainly extend the scope of processing activities, either consciously or unconsciously. As regards to this, as pointed out by the study of Domínguez Álvarez on these multiple lawful bases issue is that, the GDPR itself, in Recital 46, acknowledges that, in exceptional situations like the current one, the legal basis of processing data can be multiple, based on both the vital interest of the data subject or another natural person, and public interest.¹⁵⁷² Therefore, it is not as unusual as, it is seen at the first glance. Having said that, there could be some ambiguity appearing regarding the application of these rights granularly to the data subjects, as the users could have feeling that their data were collected and stored with many smart reasons opted by the controller, which they would be insecure about, considering the information asymmetry¹⁵⁷³ between a regular citizen and subject data controllers advised by matter experts. Therefore, eventually,

¹⁵⁷² Domínguez Álvarez, José Luis (2020) "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19." *Revista de Comunicación y Salud*, 10, no. 2, pp. 607-624, p.614.

¹⁵⁷³ As for the definition of information asymmetry, as stated by the study of arkson, Gavin; Jacobsen, Trond E. and Batcheller, Archer L. Information asymmetry arises when certain parties possess superior knowledge or information that significantly affects their ability to participate effectively in a given situation, relative to other parties involved. For the full study see arkson, Gavin; Jacobsen, Trond E. and Batcheller, Archer L. (2007) "Information asymmetry and information sharing." *Government Information Quarterly* 24, no. 4, pp.827-839, p.828.

there might not really know which single lawful basis of the processing activities are being applied to them.

On the other hand, in line with the criticism on certain other points of Radar Covid, which will be also delineated in the following Chapter, there are also ambiguity related to the other parts of the data protection aspects of the application. Certainly, we believe that we can also add this one related to the vagueness of those lawful basis to the list as well. That being said, while there is an implicit obligation of being in line with the aforementioned guidelines and legislations enacted by the respective Spanish authorities, which may also impact the classification of the lawful basis of the activities. In other words, the lawful basis of the processing activities may switch amongst article 9-2-h, 9-2-c and 9-2-l for the special categories of personal data. Hence, considering that ICO guidance on lawful basis also provided that in case controllers' purposes change, controllers can retain the ability to process data under the initial legal justification if their new purpose is in harmony and aligns with the original purpose (unless your original lawful basis was consent),¹⁵⁷⁴ therefore, such flexibility might actually have been aimed by the data controller of the application.

Accordingly, even though we might have seemed to be critical of such wide range of lawful basis, including consent, which could cause ambiguity, thereby, potential abuse for the processing activities, from the operational perspective of the application, it would evidently increase the chances of implement uninterrupted processing activities by Radar Covid, which would resulted in uninterrupted implementation of the application without any hindrance from data protection end. Similarly, many citizens in Spain, as also detailed in the referred article complained about the statement's ambiguity regarding the legal justification for the processing of personal data, as it seems contradictory. As per the view, whereas it claims that the information was given voluntarily by the user and was authorized by them to use the

¹⁵⁷⁴ ICO (2023), lawful basis for processing, available at: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing-1-0.pdf> (accessed on 23 June 2024), p.1.

application.¹⁵⁷⁵ The statement that "they will be processed for purposes strictly in the public interest in the field of public health" has been found to be too general, and this created a serious issue for the users, as per the study done by Díaz.¹⁵⁷⁶ On the other hand, the study of Domínguez Álvarez put forward the idea that, it is imperative to clarify the legal regime and the possibilities of the processing of the health data, which, as we have revealed, are essential to promote a necessary and adequate technological development to win over COVID-19. In this sense, the first thing we must point out is that the GDPR itself, in fact, recognizes that, in exceptional situations, such as the one we experienced, the legal basis for treatment may be multiple, based both on the public interest, as in the vital interest of the data subject or other person,¹⁵⁷⁷ which genuinely seems interesting and valid.

Correspondingly, from our perspective, such wide range of legal bases are also inevitably related to the legal structure of the Spanish system, as introduced above, rather than the arbitrariness or impotencies of the data controllers. To be more concrete on this reasoning, given that in Spain, health services fall under the jurisdiction and responsibility of the regions (Comunidades Autónomas).¹⁵⁷⁸ While the central government possesses the authority to establish fundamental regulations with minimum common standards and coordinate the health system, its executive powers are limited to transborder health matters, such as controls at airport entrances, as briefly touched above. Having said that, the government, which has executive power, may issue temporary legislative provisions in cases of extraordinary and

¹⁵⁷⁵ Díaz, Efrén, (2021) "Geolocation Apps Do not Cure Covid-19 They Analyze Peoples Mobility", Geospatial World, available at: <https://www.geospatialworld.net/article/geolocation-apps-do-not-cure-covid-19-they-analyze-peoples-mobility/> (accessed on 23 June 2024).

¹⁵⁷⁶ *Ibid.*

¹⁵⁷⁷ Domínguez Álvarez, José Luis (2020) "Public Administration's Challenges in Order to Guarantee the Fundamental Right of Personal Data Protection in the Post-COVID-19 Era.", *Revista Eurolatinoamericana de Derecho Administrativo*, vol. 7, núm. 1, pp. 167-191, p.178.

¹⁵⁷⁸ Nogueira López, Alba, Doménech Pascual, Gabriel "Fighting COVID 19...", *op.cit.*, p.1.

urgent need.¹⁵⁷⁹ Therefore, to get back to our main discussion here, if there is a clash between central and regional regulations on the Covid related activities, either they might be implemented or titled differently in certain regions than the central government. For instance, there has been a clash between the central government and some regions, i.e., Catalonia and Murcia, which have called for more severe quarantines, involving the cessation of construction and all industrial activities not linked to essential needs.¹⁵⁸⁰ At first, the government totally rejected some of those additional precautionary measures proposed by Murcia, and only approved very localized strict confinements such as those existing in some Catalan municipalities prior to the state of alarm.¹⁵⁸¹ Accordingly, as seen in this sample that in light of such complexity of the structure of the legal system, we believe that it would not be simply fair to treat the Spanish case based on the other samples from different countries without such complex legal structure. Hence, from this perspective, it would actually make sense to rely on the multiple lawful basis for the processing activities to prevent any sort of conflict resulted from the difference experiences arose in different regions for the management of day-to-day activities with the central government. As such, having multiple lawful basis for processing activities would facilitate the implementation of contact tracing applications, across all regions with more flexibility to apply to each legal basis, and actually it might have been deliberately placed to the privacy notice with huge number of opportunities for the controller.

On the other hand, as also briefly mentioned and criticized, it might be somewhat important to apply more specific and limited with the application's lawful basis of the processing activities due to potential user mistrust that could be create, not only in sphere of protection of their rights, but also such

¹⁵⁷⁹ Tapia, Antonia and del Campo, Amelia (2018) "Legal Systems in Spain" Thompson Reuters, [https://uk.practicallaw.thomsonreuters.com/7-634-0207?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/7-634-0207?transitionType=Default&contextData=(sc.Default)&firstPage=true) (accessed on 27 June 2024).

¹⁵⁸⁰ Nogueira López, Alba and Doménech Pascual, Gabriel (2020) "*Fighting COVID 19...*", op.cit., p.1.

¹⁵⁸¹ Nogueira López, Alba and Doménech Pascual, Gabriel, (2020) "*Fighting COVID 19...*", op.cit., p.1.

ambiguity might give a rise to other concerns which were already covered in Chapter 2. For instance, as per the study of Rich, by June, Americans' mistrust has grown, as indicated by a recent survey revealing that 71% of respondents would not use contact tracing apps, primarily due to concerns about privacy. This skepticism is fundamentally rooted in the mistrust felt by the data subject fearing tech companies and public institution for privacy reasons.¹⁵⁸²

To this end, in line with decision of AEPD, as also mentioned by Rubí Puig and Herrerías Castro¹⁵⁸³ that although privacy issues are just one of the problems identified in the development and implementation of contact tracing applications, concerns about potential violations of data protection rights are likely a major factor fueling distrust toward these new technologies, which is exacerbated with the wide range of lawful basis of processing activities, as it may invoke the idea that data controller is interested in processing users' data in as many instance as possible. Moreover, alongside the widespread mistrust of data processing carried out by public administrations, suspicions also arise regarding the involvement of the private sector in the development of contact tracing applications. In the case of Radar Covid app, the participation of well-known companies, i.e., Google, Apple, or Amazon, and rumors created could lead people to be more hesitant to download and install the application on their mobile phones,¹⁵⁸⁴ or similarly, the public's trust in organizations' ability to preserve data and their willingness to utilize it in ethically responsible ways has been damaged by the Cambridge Analytica episode and other, following to daily news about data breaches that give private information to criminals.¹⁵⁸⁵ We already delineated similar concerns Chapter 2 with regards

¹⁵⁸² Rich, Jessica (2021) "How our outdated privacy laws doomed contact-tracing apps", Brookings Institute, <https://www.brookings.edu/articles/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/> (accessed on 23 June 2024).

¹⁵⁸³ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» ...", *op.cit.*, p.272.

¹⁵⁸⁴ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» ...", *op.cit.*, p.272.

¹⁵⁸⁵ For the further details of the raised concerns see Umawing, Jovi, (2020) "Labs survey finds privacy concerns, distrust of social media rampant with all age groups", Malware Bytest, <https://www.malwarebytes.com/blog/news/2019/03/labs-survey-finds-privacy-concerns-strust-of-social-media-rampant-with-all-age-groups> (accessed on 24 June 2024).

to lack of clarity for the use of personal data by these giants going forward. Thus, as expected, experiences in other jurisdictions, where intensive tracing and tracking systems have been used, have also raised concerns.

Therefore, given that such samples are already available for the distrust of the data subjects, it is plausible to consider and implement the lawful basis of processing activities in Spain as limited as possible, which is in line with the approach brought by EDPB¹⁵⁸⁶ as well. Also, it is of huge significance to delineate such limited legal basis of processing activities and reiterate that such multiple basis will not result in those technology companies having access to personal data processed. Having said that, to tackle such misunderstandings resulted from multiple lawful bases of processing and lack of clarification on the eagerness of processing personal data by third parties, as briefly touched in Chapter 3 during the comparison of the European applications, as a positive approach of legal basis of processing, Radar Covid application strongly emphasized the use of anonymized data, i.e., anonymously communicate with the people whom data subjects contacted with¹⁵⁸⁷, in their privacy notices to diminish such concerns. In real life, therefore, this is certainly reliable feature of the application, which we believe could be interpreted in a way that despite the existence of multiple legal basis of the processing activities, data controller still seems not to be interested in the abusing such situation by using personally identifiable data of data subjects, and the controller still tried to inform users as much as possible for this positive aspect of the processing. Even though it does not necessarily mitigate the concerns related to perceived eagerness for processing activities resulted from many different lawful basis, it is at least useful to indicate by emphasizing the use of anonymized data, which should give another message to the users, namely controller is not seeking ways to abuse these

¹⁵⁸⁶ See the EDPB (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p.7.

¹⁵⁸⁷ European mHealth Hub, Radar Covid <https://mhealth-hub.org/radar-covid> (accessed on 23 June 2024).

multiple lawful basis, but rather the controller merely aim to implement contact tracing activities in Spain to tackle the pandemic.

Nonetheless, we must still remind the fact that SEDIA, alongside with Ministry of Health, was sanctioned in 2020 for breaching eight different article of the GDPR, particularly regarding article 5.1.a, which set out that processing activity should be lawful, loyal and transparent, as detailed in next chapter.¹⁵⁸⁸ Such ambiguity, from our perspective, is resulting from the vagueness of these lawful bases detailed above, which was also reiterated in the decision of the AEPD.¹⁵⁸⁹ Nevertheless, AEPD opted for reprimanding, rather than charging hefty fines on the controllers, which will be analyzed in detail in Chapter 7. In other words, despite multiple detected violations during the investigation procedure, the AEPD did not chose financial consequences on both SEDIA and DGSP.¹⁵⁹⁰ However, from a legal perspective, what we focus is the cause and trigger of the investigation implemented by the AEPD, rather than its financial or legal consequences. Therefore, such ambiguity on the lawful basis raises a concern in the eyes of the regulator as well, which was also reiterated by the national data protection supervisory authorities, such as German, Slovenian or Poland, as detailed in Chapter 3. To this end, many of the supervisory authorities published guidance and statements to prevent such ambiguity by emphasizing the importance of providing more detailed approach with advance notification to data subjects.

However, still, compared to other privacy policies detailed in Chapter 1 and 3, German, Latvian or Croatian, as some of the most elaborate ones, Radar Covid seems to be limited in terms of the details provided to the data subjects. More specifically, as per the article of Liberties, the Radar Covid's transparency increasing campaign's overall direction demonstrates the continued lack of understanding on the most effective ways to encourage fully transparent behaviors, especially with regard to open-source

¹⁵⁸⁸ See AEPD, (2021) Resolución De Procedimiento Sancionador Expediente N.º: PS/00222/2021; and AEPD, (2021) Resolución De Procedimiento Sancionador Expediente N.º: PS/00233/2021.

¹⁵⁸⁹ Resolución AEPD SEDIA, p. 210.

¹⁵⁹⁰ Resolución AEPD SEDIA, p. 210.

development.¹⁵⁹¹ Particularly, the article pointed out some problematic aspects of and transparency acts, which they found not in line with the EDPB guideline and the GDPR, which is in line with the general recommendations on the transparency document we provided in Chapter 4. As such, we are of the view that there is such ambiguity established for the lawful basis of the processing activities, and investigations as well as criticism mentioned above, such privacy policy would be at least subject to further elaboration, as an addendum. Further campaigns could also be provided related to the lawful processing activities, which would diminish the concerns raised in society, as also detailed in Chapter 4. Accordingly, like this proposition, SEDIA and Ministry of Health published a video to diminish such concerns to indicate the level of measures to be implemented by them to mitigate such concerns resulted from lack of transparency, and other concerns as well, as detailed in the next Chapter. What is more on this is that Artigas, head of the state digital and artificial intelligence unit, provided that that Radar Covid was designed with interoperability goals thereby multiple language options, as such, Artigas¹⁵⁹² concluded that “they launched the application with English option from the beginning.”¹⁵⁹³ The reason why we wanted to touch on this approach brought by the Spanish authorities is that it is certainly risk mitigation factor for foreigners residing in Spain, who cannot speak Spanish, Catalan or other official languages of the country. Even if it is a minority, it would still be a significant indicator of desire to inform users in Spain precisely, which is compatible with the GDPR and Ley Orgánica 3/2018 requirements on the notification of legal basis of processing activities. Therefore, we evaluate such actions positively, and firmly believe that such informative campaigns with understandable language options, in line with the GDPR¹⁵⁹⁴, Ley Orgánica

¹⁵⁹¹ Carrasco, Sergio (2021) “The Failure of Spain’s Radar Covid App” Liberties, <https://www.liberties.eu/en/stories/app-radar-covid-rights/43524> (accessed on 22 June 2024).

¹⁵⁹² Please refer to Carme Artigas, Head of Spain’s state digital and artificial intelligence unit.

¹⁵⁹³ See what Carme Artigas provided to Reuters, Binnia, Isla, (2020) “Spain’s COVID tracing app tries to balance public health with privacy” Reuters, <https://www.reuters.com/article/us-health-coronavirus-apps-spain-idUKKBN2680SF> (accessed on 22 June 2024).

¹⁵⁹⁴ See Article 13 of the GDPR, already mentioned.

3/2018¹⁵⁹⁵ requirements and EDPB recommendations¹⁵⁹⁶ on consent and transparency should be provided to data subjects so that they can clearly understand the legality of processing activities.

On general level, given that other data protections in different member states also emphasized the importance of transparency and lawful basis collaboration, we believe that it would not be realistic to come up with a conclusion that do not support the increase in level of clear and understandable information freed from legal jargon to the users. Although there are allegations and investigations provided on the controllers, they updated the policy and remediated the process, which we believe that in line with the goal of European perspective on data protection matters, as well as with corrective legal approach. Compared to the case with Lithuanian application, for instance, once the Lithuanian data protection authority asked the controller to halt processing of personal data by the app during its verification of the personal data handled by the app since it was crucial to determine the real extent and type of the processing activity, yet the controller erased the data instead. Hence, the controller failed to appropriately demonstrate its compliance with the guidelines by destroying the personal data handled by the app, as it did not follow the request.¹⁵⁹⁷ Nevertheless, it was not the case for the Radar Covid, and it is the positive side associated with the corrective power of the regulators.

Suitably, in summary, although there were gaps in the selection of wide range of lawful bases, as well as in the detailed indication of those bases, there are also positive acts in terms of informing people with videos, different language options and applying the early caveats of AEPD to remediate deficient aspects of the data protection matters, particularly with regards to the legality and

¹⁵⁹⁵ See Article 11 of Ley Orgánica 3/2018, already mentioned.

¹⁵⁹⁶ EDPB (2020), Guidelines on Consent, *op.cit.*, p.6.

¹⁵⁹⁷ For the decision of the State Data Protection Inspectorate (the Lithuanian Data Protection Authority) see “The Fine Issued for Infringements of the GDPR in Mobile Application “Karantinas” available at: <https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20App%20Karantinas.pdf> (accessed on 23 June 2024).

transparency of the processing activities. Additionally, quick reaction and remediation actions of the Data Controller upon certain criticisms detailed was also positive sign for the any future implementation of the applications, which indicated that Spanish authorities are capable of intervening privacy risks promptly, as addressed in AEPD decisions section of the last chapter. Hence, in line with Sanz Guedán's study, we are also of the view that, we are protected concerning the handling of our data, ensuring it cannot be used unlawfully, and there are limits to its processing,¹⁵⁹⁸ based on the inexistence of serious breaches till date. Having said that, with further consideration provided on privacy-by-design approach for the more efficient design of the application for privacy and data protection concerns should be the main focus of the controller for the legal basis of the processing activities going forward, as technicalities of the application should also be in cadence with these selections, which will also be highlighted in the last chapter.

VII. RADAR COVID AND DATA PROTECTION

1. General overview of the applications used locally and comparative analysis of Asistencia Covid-19 to Radar Covid

1.1 General overview of the local applications in Spain

Prior to delving into an in-depth exploration of the data protection facets inherent in the Radar COVID and COVID Asistencia applications, which were used on the national level, and their features, we believe that it is useful to offer a succinct overview of the array of applications employed across Spain to provide a better understanding of the entire digital tracing methods used in different regions and phases. However, it is paramount to reiterate that, in accordance with the overarching theme of this thesis, our main focus will remain on Radar COVID application, as the singular nationally endorsed contact tracing application in Spain. Therefore, this chapter will predominantly

¹⁵⁹⁸ Sanz Guedán, Sara (2021) " Geolocalización de las personas físicas en el contexto de la pandemia por la COVID 19." Universidad de Valladolid. Facultad de Ciencias Sociales, Jurídicas y de la Comunicación, <https://uvadoc.uva.es/handle/10324/48151>, pp.1-67, p.60.

concentrate on its scrutiny. Furthermore, any allusion to Asistencia COVID and other local applications will primarily serve the purpose of delineating potential privacy concerns arising from its utilization for the informatory purposes.

To begin with, in Spain, slightly different than other European Countries, in the beginning of the pandemic, there were different self-diagnosis applications available in the different regions,¹⁵⁹⁹ whose legal foundation was elaborated and assessed in the previous Chapter. To provide some detail on these applications, several apps were introduced by regional governments and public health services across Spain to address the COVID-19 crisis, such as CoronaMadrid¹⁶⁰⁰ by the regional government of Madrid, COVID-19.eus¹⁶⁰¹, by the public health service of Euskadi, STOP COVID19 CAT¹⁶⁰² by the Regional Government of Catalunya. These apps were developed with three main goals: aiding users in identifying COVID-19 symptoms and conducting self-assessments to alleviate pressure on emergency services, offering actionable information and guidance to the public, and gathering data on virus spread, including potential COVID-19 cases. More specifically, regarding COVID-19.eu, the Basque Health System (Osakidetza) collaborated with EricTel to release this app. It was provided for free as a public service, suggesting it likely does not include advertising or tracking features. Additionally, there was no indication that it incorporates geo-fencing or contact-tracing functions.¹⁶⁰³ More specifically, CoronaMadrid app, the regional government of Madrid initially introduced this mobile app as a web-

¹⁵⁹⁹ For the full technical details of the apps used in Spain, see the report prepared by AppCensus (2020) "COVID-19 Android Apps: Spain App Analysis Report", <https://blog.appcensus.io/wp-content/uploads/2020/04/report.pdf> (accessed on 27 June 2024), p.20.

¹⁶⁰⁰ Corona Madrid, Privacy Policy- (Updated) <https://coronavirus.comunidad.madrid/politica-de-privacidad/> (accessed on 27 January 2024).

¹⁶⁰¹ COVID-19.eus/Collaboro, Conditions of Use <https://colaboro.ericTEL.com/privacy/> (accessed on 27 June 2024).

¹⁶⁰² Stop Covid-19, Security Conditions <https://sem.gencat.cat/ca/061-salut-respon/apps-mobils/STOPCOVID19/condicions-seguretat/> (accessed on 27 June 2024).

¹⁶⁰³ AppCensus (2020) "COVID-19 Android Apps...", *op.cit.*, p.24.

based solution and later released it as a mobile application on March 24th, 2020,¹⁶⁰⁴ which was not a contact tracing application either. Lastly, STOP COVID19 CAT, released by the Catalan Health Service (CatSalut) on March 20th, 2020. The Catalan health service developed this app with the goals of alleviating the burden on emergency call centers and hospitals by aiding citizens in self-diagnosing based on symptoms, identifying COVID-19 patients and tracking their progress, and detecting and monitoring areas with higher infection rates.¹⁶⁰⁵ Therefore, from the public health perspective, it is plausible to state that they all wanted to achieve the same goal on the regional perspective, while they were subject to different type of technicalities and functions than contact tracing apps, thereby having varied data protection law implications due to such differences. These voluntary apps enabled users to assess their symptoms independently and subsequently offered them tailored health precautions to follow.¹⁶⁰⁶ Hence, the function of these apps was merely informative.

With regards to their infrastructure, these apps relied on cloud services such as Google Cloud (CoronaMadrid), Mubiquo's push notifications and geo-fencing services (STOP COVID19 CAT), and Amazon Web Services (STOP COVID19 CAT), and this dependence was likely aimed at expediting development and expanding their backend infrastructure.¹⁶⁰⁷ Consequently, citizens' data, including national identification numbers, location data, contact details, chronic health conditions, and COVID-19 symptoms, seemed to be stored on platforms provided by non-European companies, potentially falling under foreign legal jurisdictions. Also, these applications utilized authentication methods involving SMS text messages (two-factor

¹⁶⁰⁴ AppCensus (2020) "COVID-19 Android Apps...", *op.cit.*, p.14.

¹⁶⁰⁵ Stop Covid-19, Functional Document, p.4, and Stop Covid-19, Security Conditions, section "why do we use your data and for what purpose"

¹⁶⁰⁶ Zeng, Kylie; Bernardo, Stephanie N. and Havins, Weldon E. (2020) "The use of digital tools to mitigate the COVID-19 pandemic: comparative retrospective study of six countries." *JMIR public health and surveillance*, vol.6, no. 4, e24598, pp.1-15, p.11.

¹⁶⁰⁷ AppCensus (2020) "COVID-19 Android Apps....", *op.cit.*, p.4.

authentication) and either national identification numbers or social security numbers, different than Radar Covid.¹⁶⁰⁸ As such, the reason why we briefly delineated the nature of these applications is that main drawbacks related to these regional application were scattered around the use of geolocation, particularly for the ones that rely on it, and strong reliance on the inclusion of technology companies for the infrastructure, backend server and cloud services, and lack of transparency, which are one of the most debated aspects of Covid Asistencia and Radar Covid respectively as well. However, even if they were not contact tracing applications, they all still moved out more central processing solution, rather than relying on the regional solutions due to the privacy concerns, although autonomous regions integrated it into their own systems relatively slowly, with Madrid and Catalonia still not having done so by mid-October.¹⁶⁰⁹ Therefore, it brings a sample of approach utilized by local governments, i.e., data controllers of these short-lived applications for their risk mitigating actions upon privacy concerns, instead of insisting on the local solution. To this end, following to this high-level introduction of the other applications used on the regional level, we would like to proceed to the comparative analysis of national contact tracing application Radar Covid and symptom checker Asistencia Covid applications, from data protection law perspective to understand nuanced approach in Spain to address each specific around risks associated with the use of Radar Covid application in the following sub-chapters.

1.2 Comparative analysis of Asistencia Covid-19 to Radar Covid

In order to begin with the comparative analysis of Asistencia Covid and Radar Covid, we believe it is beneficial to draw the line between both applications in a clear manner, although it was briefly introduced in the previous chapter that Asistencia Covid offered capabilities for self-screening¹⁶¹⁰, whereas Radar

¹⁶⁰⁸ *Ibid.*

¹⁶⁰⁹ Pazos Vidal, Serafín (2021) "La dimensión territorial de la pandemia." *Informe sobre la Democracia en España 2020: El Año de la Pandemia*, pp. 171-188, p.179.

¹⁶¹⁰ Kalgotra, Pankush; Gupta, Ashish and Sharda, Ramesh (2021) "Pandemic information support lifecycle: evidence from the evolution of mobile apps during COVID-19", *Journal of Business Research*, vol. 134, pp. 540-559, p.546.

Covid designated for tracing activities. In other words, Asistencia Covid app was primarily used for obtaining information and assistance related to COVID-19, such as checking symptoms, accessing health advice, and contacting healthcare services.¹⁶¹¹ In more detail, the objective of this application, which was developed by SEDIA, was to decongest the health care telephones of the different Autonomous Communities, as stated in the resolution.¹⁶¹² Telefónica Digital Spain, SLU, undertook significant roles, and carried out the operation of activities that allowed the implementation and deployment of the app.¹⁶¹³ On the other hand, Radar Covid app was specifically designed for contact tracing and exposure notifications, which also aimed to identify potential exposures to COVID-19 by using Bluetooth technology to detect close contacts with other app users who later tested positive for the virus.¹⁶¹⁴ Having said that, both applications served complementary roles in Spain's response to the COVID-19 pandemic. Asistencia Covid provided information and support¹⁶¹⁵, as stated in its privacy policy, is to "decrease the number of calls directed to emergency health centers and resolve inquiries regarding the infectious disease COVID-19."¹⁶¹⁶ Differently, Radar Covid focused on contact tracing and exposure notifications.¹⁶¹⁷ Thus, users could choose to use one or both apps depending on their needs, without being subject to any limitation for the use thereof. Pertaining to the identity of data controllers, the data controllers were both the Ministry of Health and the Autonomous Communities.¹⁶¹⁸ Likewise, the SEDIA was in charge of the treatment.¹⁶¹⁹ On the other hand, with regards to Asistencia, even though the contact email listed on the Google Play profile belonged to ForceManager, the data

¹⁶¹¹ See Order SND/297/2020.

¹⁶¹² Resolución de 8 de mayo de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Comunidad Autónoma de Castilla-La Mancha, sobre la adhesión al uso de la Aplicación AsistenciaCOVID19, («BOE» núm. 150, de 27 de mayo de 2020, páginas 35080 a 35099 (20 págs.)) Tercero.

¹⁶¹³ «BOE» núm. 150, de 27 de mayo de 2020, Tercero.

¹⁶¹⁴ «BOE» núm. 150, de 27 de mayo de 2020, *Segunda, Características de aplicación.*

¹⁶¹⁵ See Privacy Policy of Asistencia Covid, *op.cit.*, Part 1.

¹⁶¹⁶ Aszodi, Nikolett; Galaski, Jascha; Konoplia, Oleksandra and Reich, Orsolya (2021) "COVID-19 Technology in the EU..." *Op.cit.*, p.45.

¹⁶¹⁷ See Privacy Policy of Radar Covid, *op.cit.*, Part 1.

¹⁶¹⁸ See Privacy Policy of Radar Covid, *op.cit.*, Part 3.

¹⁶¹⁹ See Privacy Policy of Radar Covid, *op.cit.*, Part 3.

controller of the application was Comunidad de Madrid¹⁶²⁰. More specifically, as detailed in the legal background in the previous chapters, in order to mitigate the potential privacy concerns resulted from the aforementioned discussions scattered around the applications in Spain, SEDIA and Ministry of Health jointly worked on the development of the application, by working in conjunction with plenty of subject matter experts and private sector companies. In other words, numerous subject matter experts collaborated to develop an application aimed at combating the coronavirus.¹⁶²¹ That being said, as detailed throughout the chapters, the involvement of third-party companies introduces potential privacy implications. Specifically, in line with the previously mentioned regional applications, several third-party private companies—including Google, Telefónica, Ferrovial, Goggo, Network, Carto, ForceManager, and Mendesaltaren—collaborated on the development of the Covid Asistencia application. Notably, the app was endorsed with a certificate issued by the Comunidad de Madrid.¹⁶²² The participation of ForceManager raised several security concerns, since in any unfortunate event that the root certificate is inadequately managed and safeguarded by the third-party responsible for the software development, a malicious actor could potentially sign and distribute software impersonating the public service.¹⁶²³ Similarly, Radar Covid application utilized third-party companies as well, which were the Apple and Google API to handle the creation, administration, and storage of these daily ephemeral identifier lists, as well as to manage Bluetooth-based interactions between mobile devices.¹⁶²⁴ In other words, Radar Covid leveraged the established GAEN infrastructure.¹⁶²⁵ Therefore, both applications, inevitable, comprised multiple third parties involved in their processing activities from data protection law perspective, more details of which will be provided and addressed in security part of this chapter. However,

¹⁶²⁰ See Privacy Policy of Asistencia Covid, *op.cit.*, Part 1.

¹⁶²¹ AppCensus (2020) "COVID-19 Android Apps....", *op.cit.*, p.20.

¹⁶²² AppCensus (2020) "COVID-19 Android Apps....", *op.cit.*, p.20.

¹⁶²³ Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes of nationally issued COVID-19 contact tracing apps: Open-source intelligence approach and content analysis." *JMIR mHealth and uHealth* 9, no. 3, e27232, pp.1-16, p.6.

¹⁶²⁴ See Privacy Policy of Asistencia Covid, *op.cit.*, part 6.

¹⁶²⁵ Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes...", *op.cit.*, p.7.

different than Radar Covid, Asistencia Covid application provided in its privacy policy that their providers and collaborators, as well as the companies they subcontract, who assist us in providing users with the application services, communicating with them, and staying in contact with them are granted access to the personal data processed by the application,¹⁶²⁶ which is not the case for Radar Covid. Particularly, to this end, the third-party developers of the application also provided that not any personally identifiable information processed, or stored, but rather the application relied on unique and anonymous code, recalled by the phones.¹⁶²⁷ In this regard, AEPD rightly advised data subjects to exercise extreme caution when identifying who, what for, and with what guarantees their personal data will be used.¹⁶²⁸ We believe this is particularly valid for such applications with multiparty development process, as it is the case for Radar Covid and Covid Asistencia application. As such, these specific circumstances, namely involvement of third parties for processing activities do automatically oblige data subjects to be more proactive and skeptic for the use of their personal data, in addition to the strict requirements that needs to be implemented by data controllers, as we addressed during chapter 3 and 4.

Subsequently, with regards to the choice of the design for Radar Covid, the SEDIA was committed to a decentralized system similar to the one recommended by the EU guidance detailed in the previous chapters.¹⁶²⁹ In more detail, the app worked by using Bluetooth to track and record encounters with other users in an unidentifiable manner, so that the central server never has access to the user's contact records.¹⁶³⁰ Thus, user logs remained strictly on users' mobile devices.¹⁶³¹ One of the most notable features was the app's

¹⁶²⁶ See Privacy Policy of Asistencia Covid, *op.cit.*, part 6.

¹⁶²⁷ See Privacy Policy of Radar Covid, *op.cit.*, Part 2.

¹⁶²⁸ AEPD (2020), Notice on coronavirus self-assessment apps and website, para 11.

¹⁶²⁹ See Privacy Policy of Radar Covid, *op.cit.*, Part 8.

¹⁶³⁰ See Privacy Policy of Radar Covid, *op.cit.*, Part 8.

¹⁶³¹ Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes...", *op.cit.*, p.7.

adherence to a decentralized approach to data management, guaranteeing that personal data stayed within users' devices.¹⁶³² It had, inevitable, plenty of implications for the rest of the processing activities, as delineated for the other European applications in chapter 3 and 4. Particularly, considering the use of geolocation by Asistencia app alleviated the concerns, considering that the most heated discussions were scattered around, the use of geolocation data for other purposes such as monitoring people's movements or complying with quarantine, which has been speculated since the application was announced as provided by the news,¹⁶³³ as provided by multiple sources of news as well. To elaborate this further, it is crucial to acknowledge that this application targeted the entire population, encompassing age groups with varying degrees of technological proficiency.¹⁶³⁴ Notably, this application being operated without the necessity of activating the user's mobile geolocation, other than the specified cases, was a distinctive feature for a tracking application.¹⁶³⁵ Radar Covid did not require location permits, as it was based on the DP3T protocol¹⁶³⁶. In other words, the platform ensured complete anonymity and abstained from geolocation usage; instead, each user is assigned a random number upon downloading the application.¹⁶³⁷ Nonetheless, it is important to highlight that it does not necessarily mean that

¹⁶³² Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes...", *op.cit.*, p.7.

¹⁶³³ For further information regarding concerns highlighted see Maldita Website, Asistencia Covid-19, la app de autodiagnóstico del gobierno, sólo te geolocaliza si la descargas y activas esta opción al empezar el test <https://maldita.es/malditatecnologia/20200406/asistencia-covid-19-app-autodiagnostico-gobiernosolo-geolocaliza-localizacion-descarga//> (accessed on 23 June 2024).

¹⁶³⁴ Romero, Mario (2020) "Covid Radar, is it Safe?", H&A Group Publications available at: <https://www.hyaip.com/en/news/covid-radar-is-it-safe/> (accessed on 23 June 2024).

¹⁶³⁵ See Privacy Policy of Asistencia Covid, part 2.

¹⁶³⁶ DP-3T Protocol developed independently by a team of more than thirty people including developers, epidemiologists and lawyers, led by Carmela Troncoso, a Spanish researcher at the Federal Polytechnic School of Lausanne, and used in other European countries such as Italy, Germany, Austria and Switzerland.

¹⁶³⁷ Gutiérrez Caballero, Patricia (2021) "Uso por la población española de las TIC. Especial importancia durante la pandemia del Covid-19", Universidad de Valladolid. Facultad de Comercio, <https://uvadoc.uva.es/handle/10324/51906>, p.26.

Radar Covid cannot access to location of the users, for example, an app may not have permission to access location data directly (the source), but it could obtain that information from the SMS outbox (the sink) as provided by the study of Sun and colleagues,¹⁶³⁸ there is still less likely to constitute a red flag from data protection law perspective within the sense of data minimization principles set out under the GDPR.¹⁶³⁹

That being said, we believe it is still worth highlighting the fact that the privacy policy of the Asistencia COVID-19 specified that geolocation was "optional" and is requested only when "registering and performing your self-assessments" in order to "connect with the health care system that corresponds to you".¹⁶⁴⁰ Therefore, it would be a bit misleading statement to provide that geolocation was active in every possible scenario of the application. Furthermore, with regards to the type of personal data collected, the differences, thereby, concerns were not limited with geolocation, but also related to the other type of processing activities. More specifically, Asistencia app forced users, for example, to accept the sending of "push" notifications which were those small messages that appeared in the top box of users' phone. Moreover, Asistencia application was also processing mobile phone number, gender, age and symptoms data, as per the detailed analysis provided by Guisado-Clavero, Ares-Blanco, and Ben Abdellah.¹⁶⁴¹ Depending on the symptoms and the data entered, the result of the evaluation would be one or the other, so recommendations could be given, and requesting the DNI

¹⁶³⁸ Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth; Camtepe, Seyit and Ranasinghe, Damith C. (2021) "An empirical assessment of global COVID-19 contact tracing applications", *IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, pp. 1085-1097, IEEE, p.1089.

¹⁶³⁹ See Article 5-1-c of the GDPR, data minimization.

¹⁶⁴⁰ See Privacy Policy of Asistencia Covid, part 2.

¹⁶⁴¹ Guisado-Clavero, Marina; Ares-Blanco, Sara and Ben Abdellah, Lubna Dani (2021) "Using mobile applications and websites for the diagnosis of COVID-19 in Spain", *Enfermedades infecciosas y microbiología clínica (English ed.)*, vol. 39, no. 9, pp.454-457.

or the date of birth was necessary to carry out this procedure from the app.¹⁶⁴² The data was intended to be retained for the duration of the health crisis or for a maximum of two years for statistical, research, or policy purposes.¹⁶⁴³ As seen, the issue of intrusive processing was not only consisting of geolocation element, contrary to what main concerns in the society raised, but also around other type of personal data processing. Particularly, as per the Privacy Policy of Asistencia, the app itself processed the following data, most of which are sensitive as per the GDPR and Ley Orgánica 3/2018 definition of sensitive personal data, namely name and surname, mobile phone number, ID / NIE, date of birth, e-mail, complete address and postal code, gender, geolocation (i.e., GPS location of your mobile phone), health data related to the symptoms users were experiencing. Specifically, due to the use of the application, the app would have also collected information about users related to the sensation of shortness of breath, fever of +37.5°C, dry cough, whether they had visited a risk zone in the last 14 days, if they had been in contact with a confirmed positive patient, or if they had nasal mucus, muscle pain, and/or general discomfort.¹⁶⁴⁴

On the other hand, with regards to the intrusiveness of Radar Covid application, individuals in society also expected the similar approach from Radar Covid application, as it was rolled out following Asistencia application, which augmented the level of fear and concern in the society. Ideally, the application appeared not to collect any personal data,¹⁶⁴⁵ although it was contested by AEPD for the pilot phase, which will be delineated in the next section of this Chapter, as it collected anonymous codes instead. The most logical explanation of this situation that everything remained anonymous during the processing activities as per privacy policy of the application, which

¹⁶⁴² Maldita, Asistencia Covid-19, la app de autodiagnóstico del gobierno, sólo te geolocaliza si la descargas y activas esta opción al empezar el test <https://maldita.es/malditatecnologia/20200406/asistencia-covid-19-app-autodiagnostico-gobiernosolo-geolocaliza-localizacion-descarga/> (accessed on 23 June 2024).

¹⁶⁴³ Aszodi, Nikolett; Galaski, Jascha; Konoplia, Oleksandra and Reich, Orsolya (2021) "COVID-19 Technology in the EU...", op.cit., p.45.

¹⁶⁴⁴ See Privacy Policy of Asistencia Covid, part 2.

¹⁶⁴⁵ See Privacy Policy of Radar Covid, part 4.

always is an efficient risk mitigant from the data protection law perspective, in line with the technical and organizational measures set out under the GDPR¹⁶⁴⁶ and Ley Orgánica 3/2018¹⁶⁴⁷ in particular. To this end, the final version of the Radar Covid seemed to comply with these necessities thoroughly. However, we must mention the fact that the previous versions of Radar Covid app and its DPIA, privacy policy, and other communications were subject to fines by AEPD, as it will be detailed in this Chapter.

Also, with regards to the storage matters of the data collected by both apps, as another main privacy concern, Asistencia ensured a mechanism that users could fill out a form to request the deletion of their data.¹⁶⁴⁸ By this, both on-request and automatic deletion option were made available to users by the controller. Furthermore, as part of the automatic deletion, the design of Asistencia indicated that the app only intended to keep and process it as long as necessary for the purposes indicated, all in accordance with the principles of data minimization and the limitation of the storage period established by applicable regulations.¹⁶⁴⁹ Once the storage period of data subjects' data concluded, it were to be deleted, anonymized, and/or blocked in accordance with the requirements established by applicable regulations.¹⁶⁵⁰ Correspondingly, we are of the view that this feature of the app has two-fold implications for data protection law. While it meets the requirement resulted from GDPR and Ley Orgánica 3/2018 for implementation of data subject's deletion requests¹⁶⁵¹, and storage limitation principles¹⁶⁵², at the same time it seems to fail to adequately implement privacy-by-design and by default approaches requested by EDPB,¹⁶⁵³ as such deletion did not take place automatically, but rather subject to the request of the data subjects. On the other hand, Radar Covid seemed to act in line with privacy-by-design and by

¹⁶⁴⁶ See Article 32 of the GDPR, security of processing.

¹⁶⁴⁷ See Article 32 of the Ley Orgánica 3/2018, security of processing.

¹⁶⁴⁸ See Privacy Policy of Asistencia Covid, part 7.

¹⁶⁴⁹ See Privacy Policy of Asistencia Covid, part 5.

¹⁶⁵⁰ See Privacy Policy of Asistencia Covid, part 5.

¹⁶⁵¹ See Article 16 of the GDPR, right to erasure ("right to be forgotten").

¹⁶⁵² See Article 4 of the GDPR, storage limitation.

¹⁶⁵³ For the full guideline see the EDPB (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

default approaches again, by aligning with the most privacy friendly option for the users namely performing its deletion periods of data on recurring intervals by default.¹⁶⁵⁴ Similarly, as provided by the privacy policy of Radar Covid app that there was certain amount of storage periods, which were elaborated accordingly.¹⁶⁵⁵ Moreover, on the top of this privacy friendly approach brought by default by the controllers of the app, it is also positive to see another facilitated mechanism for data subjects, which granted data subjects with the flexibility to uninstall the application from your device at any point. By doing so, the procedure eliminates the history of codes received from other mobile phones for close contact alert functions on your mobile phone, as clearly indicated in the privacy policy of the application.¹⁶⁵⁶ Moreover, it also fulfilled the GDPR and Ley Orgánica 3/2018 necessities by providing a room for right to be forgotten anyway, as its policy stated that data subjects were granted with several rights in relation to the data and information that the application processed, such as the rights of rectification, access, deletion, etc.¹⁶⁵⁷

Furthermore, what we found as the one of the most remarkable aspects of Radar Covid app is that as clearly delineated in the privacy policy, if users have received a positive diagnosis for COVID-19, they could actually voluntarily enter the “single-use confirmation code” in the application that will be provided to you by your Public Health Service and that will be validated on SGAD of the Ministry of Economic Affairs and Digital Transformation server. At that moment, the application would ask for their consents to send to the data controllers’ server up to a maximum of the last 14 temporary exposure keys stored on users phone, therefore, only if they provided it, these data would be sent to the SGAD server which, after to verify the accuracy of the code, they would be served to compose a daily list of temporary exposure keys of people infected with COVID-19 that are downloaded daily from the

¹⁶⁵⁴ See Privacy Policy of Radar Covid, part 7.

¹⁶⁵⁵ As per Privacy Policy of Radar Covid, Radar Covid retains temporary exposure keys and ephemeral Bluetooth identifiers on the device for 14 days before erasing them. Similarly, temporary exposure keys shared with the server by users who test positive for COVID-19 are deleted from the server after the same period. Importantly, neither these temporary exposure keys nor the ephemeral Bluetooth identifiers contain personal information or enable the identification of users' mobile phones.

¹⁶⁵⁶ See Privacy Policy of Radar Covid, part 11.

¹⁶⁵⁷ See Privacy Policy of Radar Covid, part 9.

server by all Radar COVID applications that are in operation.¹⁶⁵⁸ We believe that such approach is definitely in line with the spirit of privacy-by-design and by-default, given that it automatically approached the data subjects with the most privacy-friendly option that was possible at the time. The reason we are emphasizing the possibility of the time was that both time constraint and nature of the pandemic did not allow data controllers to act in the atmosphere, where most cutting-edge privacy technology were applicable, due to the urgency and unexpectedness. Hence, in general, we are pleased to see a room for implementation of data subject requests for both applications. That being said, the design of Radar Covid seems to be more in line with the GDPR¹⁶⁵⁹ and Ley Orgánica 3/2018¹⁶⁶⁰ principles in terms of prevention of intrusive processing activities implemented by data controllers, due to processing via Bluetooth and anonymized data, as well as based on their privacy policies, terms and conditions, and technical details provided. In any case, as detailed above, we should not forget the fact that both applications served for different purposes. Therefore, it would not entirely be fair to compare both applications from the same data protection lens, given the nature of processing, in line with purpose of processing activities set out in the EDPB and AEPD guidelines. In the following sections of this Chapter, in line with the goal of the research, we will address the general implementation of Radar Covid application from user acceptance perspective, which automatically correlates to the security concerns pertaining to the Radar Covid, which will be addressed subsequently, and the AEPD's verdict on the data controllers of Radar Covid applications from data protection law perspective.

2. Implementation of Radar Covid

As detailed in the previous Chapter, in the realm of pandemic management within the intricate framework of the Spanish legal system, the evaluation of digital contact tracing applications in Europe has unveiled a nuanced

¹⁶⁵⁸ See Privacy Policy of Radar Covid, part 2.

¹⁶⁵⁹ See Article 24 of the GDPR, data controller responsibilities.

¹⁶⁶⁰ See Article 24 of Ley Orgánica 3/2018, data controller responsibilities.

landscape. As this chapter unfolds, our focus converges on a detailed exploration of the Radar Covid application, and its implementation from data protection perspective. A solid example of necessary coexistence between technological development and the safeguarding of the fundamental right to personal data protection is found in the implementation of the Radar Covid application, which, despite its late deployment, aims to be an essential tool in the hands of health authorities to finally control the spread and extension of the health pandemic.¹⁶⁶¹ Many people tend to mention efficiency concerns, when it comes to the implementation. For some, the effectiveness and utility of the application are closely and directly linked to its full and responsible use by citizens, a matter in which media and communication professionals acquire transcendent importance, becoming indispensable agents in providing accurate and truthful information to the entire population.¹⁶⁶² However, as mentioned by Carnovale and Khahlil as well, defining efficacy poses a challenge and can vary in different situations. Certain public health authorities may gauge the apps' efficacy based on their capacity to decrease the overall infection spread compared to manual contact tracing.¹⁶⁶³ Alternatively, some may also define it more narrowly, focusing on the ability to identify and notify more individuals about potential exposures than manual contact tracers could achieve.¹⁶⁶⁴ Or similarly, as provided by the study of Ezzaouia, and Bulchand-Gidumal in which they examined the determinants of users' intentions to use the apps, suggests that the expected advantages of using CTA have the potential to enhance users' willingness to embrace such applications.¹⁶⁶⁵ Additionally, factors such as accuracy, ease of use, and social influence hold

¹⁶⁶¹ Domínguez Álvarez, José Luis (2020) "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19." *Revista de Comunicación y Salud* 10, no. 2, pp. 607-624.

¹⁶⁶² Domínguez Álvarez, José Luis. "La necesaria protección ...", *op.cit.*, p.624.

¹⁶⁶³ Carnovale, Maria, and Louisy, Khahlil (2021) "Public Health, Technology, and Human Rights: Lessons from Digital Contact Tracing." *arXiv preprint arXiv:2107.07552*, pp.1-23, p.11.

¹⁶⁶⁴ Carnovale, Maria, and Louisy, Khahlil (2021) "Public Health, Technology, and Human Rights...", *op.cit.*, p.11.

¹⁶⁶⁵ Ezzaouia, Imane, and Bulchand-Gidumal, Jacques (2021) "A Model to Predict Users' Intentions to Adopt Contact-Tracing Apps for Prevention from COVID-19", *Information and Communication Technologies in Tourism 2021: Proceedings of the ENTER 2021 eTourism Conference, January 19–22, 2021*, pp. 543-548. Cham: Springer International Publishing, 2021, p.547.

significance, with perceived value, safety, and privacy perception following suit in importance ¹⁶⁶⁶. Therefore, as seen there are plenty of factors and determinants pertaining to the success criteria of the implementation of the apps. Nevertheless, we define our efficiency of the implementation as putting the necessary safeguards and transparency to mitigate data protection law related concerns of the users, which, as discussed in previous chapters, plays a significant role in the user acceptance, which will be detailed across this section.

As such, first of all, we must call out the fact that the public response to Radar Covid application was mixed with varying levels of adoption across different regions of the country, some of which were alleviated by the security issues addressed below. The main reason is that the choice of technological features, data management approach, and communication strategies significantly influence the public response and adoption rates, as also reiterated in previous Chapters. Accordingly, Spain, with %15 of total populations' download rate, was one of the worst in entire Europe, as per the data shared in the study of Kozyreva and colleagues,¹⁶⁶⁷ and %18 figure as one of the worst performers in terms of the downloads was also presented by the EU Commission's data.¹⁶⁶⁸ It is, therefore, showing us that user acceptance rate was significantly low compared to other countries, such as Germany, Finland or the UK. Similarly, the study of Gutiérrez Caballero also indicated this view by providing that the application did not achieve the anticipated acceptance as less than 2% of the over 3 million detected infections in Spain have been reported through this application.¹⁶⁶⁹ Thus, we are of view that assessing the direct impact of Radar Covid on curbing transmission rates proved to be complex and dependent on the countries

¹⁶⁶⁶ Ezzaouia, Imane, and Bulchand-Gidumal, Jacques (2021) "A Model to Predict Users' Intentions...", *op.cit.*, p.547.

¹⁶⁶⁷ Kozyreva, Anastasia; Lorenz-Spreen, Philipp; Lewandowsky, Stephan; Garrett, Paul M.; Herzog, Stefan M.; Pachur, Thorsten and Hertwig, Ralph (2021) "Public perceptions of COVID-19 digital contact tracing technologies during the pandemic in Germany", *OSF*, osf.io/xvzph, pp.1-61, p.38.

¹⁶⁶⁸ European Commission (2022) Digital Contact Tracing Study on lessons learned, best practices...", *op.cit.*, p.69.

¹⁶⁶⁹ Gutiérrez Caballero, Patricia. (2021) "Uso por la población española de las TIC...", *op.cit.*, p.26.

included in the comparison, but it still can provide a meaningful indication for the data subjects' behavior.

However, we do also believe that given that it was one of the most populated countries of the European Union, the user acceptance should also be in line with this figure to tackle the pandemic efficiently, this was either related to the implementation of the data protection campaign of the application itself, or to data protection and privacy failures in the form of security weaknesses resulted from the app. In this section, we will focus on implementational implications, whereas in the next section, we will also analyze security issues. Accordingly, we must mention the fact that the main drawback associated by this situation was that traditional surveillance methods can often miss a significant portion of new infections during the early stages of a disease outbreak.¹⁶⁷⁰ This was evident with Covid, where many cases went undetected initially due to limitations in testing capacity, the novelty of the virus, and asymptomatic cases.¹⁶⁷¹ This situation led to a substantial number of undocumented infections, which in turn made it challenging to grasp the true extent of the spread and implement effective control measures promptly. On the other hand, there were also concerns raised by the healthcare sector on relation to the apps is whether the app could trigger avalanches of false close-contacts leading to an avalanche of false positives that could overwhelm primary healthcare resources.¹⁶⁷² Hence, we believe that this part of the discussion regarding the implementation of the application is out of our main theme of research, and probably requires further research.

As such, what we can provide on this discussion is to discuss the wider user acceptance by mitigating privacy concerns in Spain, as we provided for other

¹⁶⁷⁰ Rodríguez, Jorge P.; Aleta, Alberto and Moreno, Yamir (2023) "Digital cities and the spread of COVID-19: Characterizing the impact of non-pharmaceutical interventions in five cities in Spain", *Frontiers in Public Health*, vol.11, 1122230, pp.78-88, p.9.

¹⁶⁷¹ *Ibid.*

¹⁶⁷² Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment", *op.cit.*, p.591.

European countries in the previous chapters as well. We agree with the perspective provided by the study of Raman and colleagues that extensive advertising campaigns and interventions related to COVID-19, along with contact tracing applications, have been demonstrated to enhance the acceptability of the application.¹⁶⁷³

Interestingly, this characteristic appears to be independent of geography, socioeconomic development, or the type of government.¹⁶⁷⁴ To this end, we are of the view that, compatible with our approach throughout the chapters, Spanish authorities actually made efforts to build public trust by promoting transparency in app development, emphasizing privacy protection, and providing clear information about data handling.¹⁶⁷⁵ The majority of autonomous communities in Spain embraced the Radar Covid app subsequent to the conclusion of COVID-19 testing in various regions by the end of August.¹⁶⁷⁶ Particularly, in line with our proposal in Chapter 4, Spanish controller provided detailed risk analysis¹⁶⁷⁷ and DPIA¹⁶⁷⁸, although with slight delay upon AEPD's caveats, as detailed in respective section of this Chapter. In these documents, both the Ministry of Economic Affairs and Digital Transformation and SEDIA indicated potential risky scenarios for processing

¹⁶⁷³ Raman, Raghu; Achuthan, Krishnashree; Vinuesa, Ricardo and Nedungadi, Prema (2021) "COVIDTAS COVID-19 Tracing App Scale-An Evaluation Framework", *Sustainability*, vol.13, no. 5, pp. 1-19, p.11.

¹⁶⁷⁴ Raman, Raghu; Achuthan, Krishnashree; Vinuesa, Ricardo and Nedungadi, Prema (2021) "COVID-19 Tracing App Scale...", *op.cit.*, p.11

¹⁶⁷⁵ Kyotu Technology Report (2020) "Unveiling the impact of covid tracking apps around the globe" <https://www.kyotutechnology.com/unveiling-the-impact-of-covid-tracking-apps-around-the-globe/> (accessed on 23 June 2024).

¹⁶⁷⁶ Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes....", *op.cit.*, p.8.

¹⁶⁷⁷ For full risk assessment see "Análisis de Riesgos Sistema de Información Radar Covid-19" available at: <https://rightsinternationalspain.org/wp-content/uploads/2022/03/Ana%CC%81lisis-de-riesgos-agosto-2020.pdf> (accessed on 23 June 2024).

¹⁶⁷⁸ For the full DPIA see "Informe de Evaluación de Impacto relativa a la Protección de Datos Tratamiento Radar Covid" available at: <https://rightsinternationalspain.org/wp-content/uploads/2022/03/Informe-de-Evaluacio%CC%81n-de-Impacto-relativa-a-la-Proteccio%CC%81n-de-Datos-Tratamiento-Radar-COVID.pdf> (accessed on 23 June 2024).

activities¹⁶⁷⁹, and delineated the risk treatment plan, action plan and targeted risk amount in detail as well.¹⁶⁸⁰ Accordingly, despite the massive criticism related to lack of info on DPIA, the updated version of DPIA was also positive in the sense of indicating technical and organizational safeguards envisaged by data controller. It seemed to delineate the important parts provided by AEPD Guideline on risk management and impact assessment in processing activities, in terms of estimating level of risk, detailing security measures in place, data protection by design and default, transparency and rights as risk reduction measures.¹⁶⁸¹ That being said, as rightly pointed out by the research of Roig Batalla that existence of DPIA prior to the deployment of the application could have contributed to a better understanding of the application by users¹⁶⁸², which we believe is not only a statement for complying with the risk identification necessities, but also for the transparent indication of such proactive approach against the risks as detailed in previous sections.

Suitably, in this point, we also agree with the thought of Velicia-Martin and colleagues, who provided that users, particularly employed ones, would be inclined to use the app if they trust it and perceive it as valuable, respectful, and easy to use, with privacy concerns having minimal influence on their intention to use it,¹⁶⁸³ which we provided through the chapters for the European applications as well. Similarly, the statistics pertaining to the adoption of the app indicated that as of July 2020, only a limited number of

¹⁶⁷⁹ See "Informe de Evaluación de Impacto relativa a la Protección de Datos..." op.cit., Plan de Acción o de tratamiento de riesgos, p.26.

¹⁶⁸⁰ See "Informe de Evaluación de Impacto relativa a la Protección de Datos..." op.cit., Evaluación De Riesgos Y Salvaguardas, p.22.

¹⁶⁸¹ For the full Guidance see AEPD (2021) "Risk management and impact assessment in processing activities" available at: <https://www.aepd.es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf> (accessed 23 June 2024).

¹⁶⁸² Roig Batalla, Antoni (2021) "Garantías frente a las aplicaciones de rastreo de contagios en situaciones de pandemia." *Teoría y realidad constitucional*, 48, pp. 527-542, p.534.

¹⁶⁸³ Velicia-Martin, Felix; Cabrera-Sanchez, Juan-Pedro; Gil-Cordero, Eloy and Palos-Sanchez, Pedro R. (2021) "Researching COVID-19 tracing app acceptance: incorporating theory from the technological acceptance model", *PeerJ Computer Science*, vol.7, e316, pp.1-20, p.5.

citizens installed the app on their mobile devices due to the social mistrust associated with such technology.¹⁶⁸⁴ Within the similar vein, one interesting takeaway could be derived from the study of EU Commission.¹⁶⁸⁵ As per the results of the research implemented, Radar Covid is the second application that attracted most tweets by individuals. We believe that, given the timing of these tweets, i.e. first days of the application becoming available, critically shows the reaction it yielded from the individuals in society. To solidify the approach, 90% of these tweets were in Spanish, and 4% were in Catalan.¹⁶⁸⁶ Therefore, from our perspective, although it is not the sole indicator, we believe that people in society took this topic very unusually, which may provide us with the understanding of heated concerns related to privacy matters. To solidify this approach in Spain, also study of Kamalova, and Moralejo called out the similar outcome with different method by pointing out that approximately half of the news on contact tracing topic addresses its impact on user privacy in some way.¹⁶⁸⁷ The percentage of news articles addressing privacy positively is much lower than in Spanish media (42.9%) and is very similar to those that address it in a neutral manner (38.1%). Nearly one in five news articles presents a negative view of Radar Covid's privacy.¹⁶⁸⁸ As such as seen, the user concern, seem to play an important role in Spain as well, like the other countries we have discussed in previous Chapters.

To this end, we also believe that study of Rodríguez and their colleagues is valuable for our research, as overall results of the controlled experiment study were positive and we can conclude that, a priori, after suitable communication campaigns, it could potentially achieve a satisfactory level of adoption and

¹⁶⁸⁴ Nieto Garrido, Eva María (2021) "Risks for the fundamental right...", *op.cit.*, p.281.

¹⁶⁸⁵ The European Commission, (2020) Analysing mobile apps that emerged to fight the COVID-19 crisis, p.25.

¹⁶⁸⁶ The European Commission (2020) Analysing mobile apps that emerged to fight the COVID-19 crisis, p.26.

¹⁶⁸⁷ Kamalova, Sofiya, and Alfredo Moralejo.(2022) "El tratamiento periodístico de la privacidad en las aplicaciones de rastreo de COVID-19 en España y Reino Unido." *Dígitos: Revista de Comunicación Digital*, ISSN-e 2444-0132, N°. 8, 2022, pp.215-230, DOI: [10.7203/drdcd.v1i8.222](https://doi.org/10.7203/drdcd.v1i8.222), p.222.

¹⁶⁸⁸ Kamalova, Sofiya, and Alfredo Moralejo (2022) "El tratamiento periodístico ...", *op.cit.*, p.222.

compliance, making it a valuable supplement to manual contact tracing and other non-pharmaceutical interventions in containing epidemic outbreaks, thereby justifying its nationwide implementation.¹⁶⁸⁹ Within the same remit, we are also of view that, in line with what we have already provided on the significance of information campaigns to ensure the transparency by Spanish controller, the study of Ussai and colleagues provided the similar approach for Italian controller. In more detail, their study concluded that the adoption of digital contact tracing apps might be hindered by various perceived risks, such as privacy concerns, especially if these risks are not offset by clearly communicated benefits to the population.¹⁶⁹⁰ Authorities have demanded elevated levels of transparency throughout the establishment of digital contact tracing tools, which includes proactive communication addressing ethical, legal, and social concerns associated with such technologies before their introduction.¹⁶⁹¹ As such, no doubt, as also reiterated by the study of José Luis Domínguez Álvarez that the role of the media and communication professionals becomes crucial in informing the public about the advantages and potential benefits of using the Radar Covid app responsibly and fully.¹⁶⁹² We believe that by this, users can be more efficiently informed about pinpoint benefits of the applications, which would tackle all the ambiguities and concerns delineated in Chapter 2 for user's concerns. Hence, in light of these

¹⁶⁸⁹ Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment assessing the epidemiological impact of digital contact tracing", *Nature Communications*, vol. 12, no. 1, pp.1-6, p.4.

¹⁶⁹⁰ Ussai, Silvia; Pistis, Marco; Missoni, Eduardo; Formenti, Beatric; Armocida, Benedetta; Pedrazzi, Tatiana; Castelli, Francesco; Monasta, Lorenzo; Lauria, Baldassare and Mariani, Ilaria (2022) "Immuni" and the National Health System: Lessons Learnt from the COVID-19 Digital Contact Tracing in Italy", *International Journal of Environmental Research and Public Health*, vol. 19, n.12, 7529, pp.1-7, p. 6.

¹⁶⁹¹ Ussai, Silvia; Pistis, Marco; Missoni, Eduardo; Formenti, Beatric; Armocida, Benedetta; Pedrazzi, Tatiana; Castelli, Francesco; Monasta, Lorenzo; Lauria, Baldassare and Mariani, Ilaria (2022) "Immuni" and the National Health System...", *op.cit.*, p.6.

¹⁶⁹² Domínguez Álvarez, José Luis (2020) "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19", *Revista de Comunicación y Salud*, vol.10, no. 2, pp. 607-624, p.619.

different inputs on the interplay between the user acceptance and transparency campaigns particularly regarding the legal and data protection law related aspects of the application, looking at the transparency acts and campaigns of Spanish data controller seemed to be the right direction of the travel to determine the implementation of the application.

Subsequently, another positive approach brought by the controller in relation to the transparent approach that once the application was downloaded, the user was asked to accept the terms of use and the privacy policy,¹⁶⁹³ both of which, we believe, were sufficiently detailed to give a proper understanding of processing activities from transparency perspective. This, certainly, an important factor to comply with the required level of transparency and clarity expected from data controller within the context of data protection laws and transparency laws in Spain.¹⁶⁹⁴ In addition to this, not only such detailed privacy policy and terms of use were provided to the users, but also controllers released a video titled "What does Radar Covid not do?" as part of promotional efforts for Spain's contact-tracing application. The video clarified that despite navigating the country's decentralized healthcare system, the app does not track users' locations, identify them, record personal information, or transmit data¹⁶⁹⁵. We believe that it is positive in many senses, as it solidifies the users' understanding of the existence of most privacy friendly version of the application in a short, understandable and concise way, in line with the EDPB transparency requirements.¹⁶⁹⁶ Lastly, it is important to communicate the users in terms of these technical and organizational safeguards

¹⁶⁹³ Mendoza García, María Pilar (2021) "Protección de datos y herramientas tecnológicas para la prevención del Covid-19: análisis a la luz de dos modelos contrapuestos (España vs Emiratos Árabes Unidos)." *Repositorio institucional de la Universidad de Cantabria* G1765 Trabajos académicos, 692, pp.1-38, p.22.

¹⁶⁹⁴ For the referred legislation on transparency see Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE núm. 295, de 10/12/2013).

¹⁶⁹⁵ Binnia, Isla (2020) "Spain's COVID tracing app tries to balance public health with privacy" Reuters, <https://www.reuters.com/article/us-health-coronavirus-apps-spain-idUKKBN2680SF> (accessed on 23 June 2024).

¹⁶⁹⁶ See the EDPB (2018) Guidelines on transparency under Regulation 2016/679, p.6.

implemented by the application, as also provided for the previous chapters. Such approach would be compatible with the privacy-first approach, as users would be able to see and understand all sort of safeguards in place. For instance, as solid indication of such necessity could be found in the implementation of data controllers for securities in place. More specifically, as Sanz Guedán mentioned that on the main screen after the installation, there were two boxes with relevant information, namely concerning the box labeled "my data," it gave a summary of the application's privacy, explaining that it did not collect any personal data or geolocation information. Therefore, it was indicated to the users that neither our identity nor that of other people we've been in contact with can be determined.¹⁶⁹⁷ The box labeled "Radar Covid statistics" provided some interesting data to understand the app's usage.¹⁶⁹⁸ At the first glance, it might not seem to be an efficient risk mitigant, or detailed communication. Nevertheless, from our perspective, what Sanz Guedán pointed out is actually quite a pinpoint to this matter, as it is a short and understandable form of message conveyed to data subject users on their protected privacy and data protection rights. One more time, it is beneficial to reiterate that any transparent communication must be understandable, and provided in concise language.¹⁶⁹⁹ In more detail, to support this approach, we found the perspective brought by Splinter and colleagues that when creating an application and crafting its content, it is crucial to take into account its accessibility for people with limited literacy levels.¹⁷⁰⁰ Hence, providing people with the message of their data is not subject to geolocation or any processing should be provided as simple and understandable as possible. If possible, the most straightforward words should be selected for describing exactly what we

¹⁶⁹⁷ Sanz Guedán, Sara (2021) "Geolocalización de las personas físicas..." op.cit., p.60.

¹⁶⁹⁸ Sanz Guedán, Sara (2021) " Geolocalización de las personas físicas..." op.cit., p.60.

¹⁶⁹⁹ See the EDPB (2018) Guidelines on transparency under Regulation 2016/679, p.6.

¹⁷⁰⁰ Splinter, Bas; Saadah, Nicholas H.; Chavannes, Niels H.; Kiefte-de Jong, Jessica C. and Aardoom, Jiska J. (2022) "Optimizing the Acceptability, Adherence, and Inclusiveness of the COVID Radar Surveillance App: Qualitative Study Using Focus Groups, Thematic Content Analysis, and Usability Testing", *JMIR Formative Research*, vol. 6, no. 9 e36003, pp.1-15, p.13.

have been pointing from the beginning to solidify data subjects' trust for the wider user acceptance.

However, we must also remind the fact that such centralized transparency campaigns pertaining to the data security, data protection and privacy of the applications should always be supported on AC level too, considering that whereas Radar Covid serves as a nationwide contact tracing app, operating within Spain's decentralized healthcare system where responsibilities are delegated to each autonomous community,¹⁷⁰¹ and each AC had to integrate the app with its individual contact tracing system to enable its functionality.¹⁷⁰² Accordingly, each AC should sync their privacy campaigns as per the central version disseminated to the data subjects through various channels, so that there is a consistent and efficient amount of communication mitigating the concerns around data protection. Correspondingly, it is positive to observe that aforementioned necessities are implemented by data controllers on central level, yet, still, there is a further consideration required as to whether public authorities of AC should sync their campaigns with the central government. Accordingly,

Lastly, while implementing the applications, in addition to solid transparency campaigns, and publicly accessible risk assessment, we also believe that principle of necessity and proportionality in the sense of the GDPR¹⁷⁰³ should

¹⁷⁰¹ Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment..." op.cit., p.4.

¹⁷⁰² Dubin, Kenneth A. (2021) "19 Spain's response to Covid-19", *Coronavirus Politics*, pp.339-260, p.343.

¹⁷⁰³ See the EDPS definition for necessity and proportionality which states that assessing the restriction of fundamental rights, such as the right to personal data protection, relies on the principle of necessity, which holds significant importance according to legal precedent. Given the pivotal role personal data processing plays in various fundamental rights, any limitation on the right to data protection must be strictly necessary. This necessity must be substantiated by objective evidence and serves as the initial step before evaluating the proportionality of the restriction. Proportionality, a cornerstone of EU law, governs the exercise of authorities' powers by demanding a balance between means and objectives. Particularly concerning fundamental rights like personal data protection, proportionality is paramount

be prioritized for the implementation of the application as well. In other words, we are of the view that what Ramiro provided is in line with our approach for the necessity of proportionality and safeguards for the implementation of contact tracing activities.¹⁷⁰⁴ Accordingly, their study concluded how these control measures could easily comply with the principles outlined in the GDPR regarding data minimization, specific purpose, predetermined retention period, and transparency in all aspects, ensuring the anonymity of the subjects, which, we believe, is in line with the fact that there has not been any drastic personal data breach other than certain concerns raised by citizens during the first deployment of the application. Nevertheless, Ramiro also pointed out the fact that the use of contact tracing measures must be addressed not only for its implications but also from an ethical perspective, both regarding the method used in handling personal data, especially sensitive data, and the intended objectives, results, and potential discriminatory effects.¹⁷⁰⁵ As these measures, to some extent, limit rights and represent a form of citizen surveillance (especially the apps), the possibility of misuse should be considered, adopting measures to prevent this and protect not only the fundamental right to data protection but also other fundamental rights that could be affected. On the positive side, as suggested by Ang, Vincent, and Lwin Khin Shar study that the privacy-by-design approach of the Google Apple Exposure Notification (GAEN) framework restricts the amount of data collected, which can present challenges for contact tracing efforts to

in any restriction imposed. Specifically, it mandates that the benefits gained from limiting the right do not outweigh the drawbacks of its exercise, requiring a justified limitation. For the full definitions see the EDPS Website Necessity and Proportionality available at: https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en#:~:text=In%20the%20context%20of%20fundamental,disadvantages%20to%20exercise%20the%20right. (accessed on 18 February 2024).

¹⁷⁰⁴ Arenas Ramiro, Monica (2021) "Nuevas tecnologías y retos para la protección de datos personales en Europa: el rastreo de contactos durante la pandemia por covid-19." *Confluências| Revista Interdisciplinar de Sociologia e Direito*, vol.23, n. 2, pp. 99-17, p.113.

¹⁷⁰⁵ Arenas Ramiro, Monica (2021) "Nuevas tecnologías...", *op.cit.*, p.114.

swiftly determine the transmission chain.¹⁷⁰⁶ Consequently, some countries like Singapore opted not to adopt the GAEN framework, deeming it less effective within their local context.¹⁷⁰⁷ Nonetheless, from the data protection level, it seems to fulfil all necessary requirements as per the GDPR and Ley Orgánica 3/2018, as also detailed across the Chapters, such as ensuring non-identification of data subjects, usage of Bluetooth, decentralized processing and limited amount of storage of non-identifiable data. Nonetheless, from technical standpoint, there is a need for further research as to whether such promises were fulfilled within the technical sense as well. That being said, given that nothing has provided on the contrary till date, what we can provide, in line with the main concern of our thesis, is that implementation of privacy-by-design approach by data controllers brings an efficient tool to support the implementation of the application to reduce the risk levels to certain degree, providing that it does not impede the efficient tracing.

Correspondingly, it is positive to observe that Spanish application was also designed with purposes of interoperability, as also cited in Chapter 6.¹⁷⁰⁸ In more detail, Radar Covid also shared data across a network with similar apps from ten other European countries: Germany, Belgium, Croatia, Denmark, Finland, Italy, Ireland, Latvia, the Netherlands, and Poland.,¹⁷⁰⁹ which we believe it was a significant feature to bolster entire EU's defense against Covid, whereas at the same time supporting Spanish citizens and residences healthcare as well, from the general implementation perspective. As rightly pointed out by the study of Jimenez, the functioning of these systems was quite similar; in the case of Radar Covid, the app stands out for two

¹⁷⁰⁶ Ang, Vincent, and Lwin Khin Shar. (2021) "Covid-19 one year on—security and privacy review of contact tracing mobile apps." *IEEE Pervasive Computing* 20, no. 4, 61-70, p.64.

¹⁷⁰⁷ Ang, Vincent, and Lwin Khin Shar. "Covid-19 one year on—security ...", *op.cit.*, p.64.

¹⁷⁰⁸ See what Carme Artigas, Head of Spain's state digital and artificial intelligence unit provided in Binnia, Isla,(2020) "Spain's COVID tracing app tries to balance public health with privacy", Reuters Website Article, available at: <https://www.reuters.com/article/idUSKBN2680SE/> (accessed on 23 June 2024).

¹⁷⁰⁹ Villaplana Jiménez, Francisco Ramón (2021) "Recursos digitales de colaboración y de seguridad pública. Mejorando la autoprotección ciudadana", *RIPS: Revista de Investigaciones Políticas y Sociológicas*, vol. 20, no. 2, pp.1-18, p.13.

functionalities: first, identifying if someone has been in contact with an infected person in recent days; and second, anonymously notifying the app about one's positive diagnosis. Therefore, we believe that from the compatibility perspective, the entire logic of the applications is not differing from each other, there is nothing much to cover here.

Nevertheless, from our angle, it is also important to remember a significant blocker for the implementation of interoperable applications, namely late deployment and incompatibility of the structure of the apps, considering, as called out by Pazos-Vidal that the autonomous communities integrated it into their own systems very slowly, with Madrid and Catalonia still not having done so by mid-October.¹⁷¹⁰ Moreover, the inclusion of multiple countries, even if they are EU countries as well, might have raised concerns pertaining to the unauthorized access to the personal data of users by different technology firms and governmental organizations, which is of similar nature to the discussions we have tried to address within the realm of third party access to the personal data. However, on the top of that we would like to point put forward by Jiménez that the Spanish government could not be able to launch Radar Covid app until August, as there were significant concerns about big data and data protection rights, whereas different governments have persisted in recommending their use as a necessary safety measure against the coronavirus, assuring that personal data would be treated anonymously.¹⁷¹¹ Similarly, Rubi Puig and Herrerías Castro also provided that the Spanish government acted quickly but not as promptly as other states.¹⁷¹² Given the volume of reaction provided by the data subjects, our view is that this should not be interpreted in isolation from the other determinants in place, yet, we should be vary of a need to deep dive into the sociological and data protection law related differences. The first one does not fall within the scope of our research, so we must defer it to other colleagues. That being said, in relation to the regulatory aspects and any potential red flags which might have

¹⁷¹⁰ Pazos Vidal, Serafín (2021) "La dimensión territorial de la pandemia." *Informe sobre la Democracia en España 2020: El Año de la Pandemia*, pp. 171-188, p.179.

¹⁷¹¹ Villaplana Jiménez, Francisco Ramón. (2021) "Recursos digitales de colaboración.", *op.cit.*, p.13.

¹⁷¹² Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "«COVID Radar» and protection...", *op.cit.*, p.243.

triggered people's concerns towards the application, as also detailed in previous chapters for the other applications, and next section of this chapter for the Spanish app, significance of transparent communication on the existence of potential risks, and all of the risk mitigants conducted by data controller of the app, and most importantly overarching benefits of using these applications must have been clearly indicated. In other words, problems related to the lack of details in privacy policy of the app, or lack of DPIA as raised by AEPD for the pilot version, which were detailed in this chapter might actually have exacerbated these concerns that did seem to have an impact on the user acceptance of the application.

Therefore, in summary, the solutions we recommended for other European applications in Chapter 4 in privacy-by-design and privacy-by-default could be easily leveraged to Spanish Radar Covid app as well. To solidify our stance on this matter, we can refer to the words of Dr. Lacasa¹⁷¹³ added, even though the app's privacy measures benefit users, they significantly restrict the data they can gather to properly evaluate its effectiveness. While their findings show great potential, they must be approached carefully, and more investigation is necessary to grasp how using the app influences behavior.¹⁷¹⁴ Therefore, although it is not the main impediment generated by the stringent privacy-by-design approach, it is indirectly impacted by the same notion for the analysis of the success of digital contact tracing applications. For instance, due to the same reason, the calculated quantity of contacts traced digitally per initial infection is a generalized indirect estimate; they did not cover the entire range and consequently lack dispersion data.¹⁷¹⁵ We, nevertheless, still believe that the essence of privacy-by-design is not only related to applying most stringent technical safeguards from the feature, but also understanding

¹⁷¹³ One of the authors of full version of Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment assessing the epidemiological impact of digital contact tracing", *Nature Communications*, vol.12, no. 1, pp. 1-6.

¹⁷¹⁴ Queen Mary University (2021) "Study Provides First Real-World Evidence of COVID-19 Contact Tracing App Effectiveness" available at: <https://medicalxpress.com/news/2021-01-real-world-evidence-covid-contact-app.html> (accessed on 22 December 2023).

¹⁷¹⁵ Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment", *op.cit.*, p.4.

the purpose of the processing activities and adapting the measures accordingly, by allowing the coexistence of both privacy and implementation of the purpose. Therefore, as provided by us through the chapters of this thesis that data controllers and any potential third parties involved in development phase of these applications must do their best to justify and document this balance targeted.

Overall, we can conclude that implementation of the app from data protection and transparency perspective did not seem to fail, due to the aforementioned reasons. Nevertheless, we must reiterate that this study has been merely focused on data protection law aspects of the implementation, whereas there is further research needed for the implementation from healthcare efficiency or ethical perspective to fully investigate the efficiency, which does not fall within the scope of this section. Furthermore, security issues are another determinant associated with the successful implementation of the application from data protection law perspective, which is analyzed and elaborated in the next section of this chapter.

3. Security Issues of Radar Covid

Data security matters, in addition to the above-mentioned organizational measures, are one of the most crucial topics to address to implement efficient data protection law compliance and solidify the data controllers' reputation, thereby achieving user trust as briefly mentioned in the previous section as well. To support our perspective on this one, what the study of Kozyreva and colleagues provided cautiously delineated the importance of data security matters within the scope of digital contact tracing activities. Their study Their research highlighted the critical importance of trust in government and the app's security, along with concerns regarding the app's effectiveness.¹⁷¹⁶ The tension between altruistic motives and personal gains, contrasted with skepticism about data security and the app's efficacy, significantly influences individuals' decisions regarding the adoption of digital contact-tracing

¹⁷¹⁶ Kozyreva, Anastasia; Lorenz-Spreen, Philipp; Lewandowsky, Stephan; Garrett, Paul M.; Herzog, Stefan M.; Pachur, Thorsten and Hertwig, Ralph (2021) "Public perceptions of COVID-19 digital contact tracing", *op.cit.*, p.3.

technologies.¹⁷¹⁷ Within the similar vein, we can also point out to the study of Sun and colleagues, which provided that over 55% of participants express extreme concern about the accuracy of tracing apps, while over 49% harbor similar levels of apprehension regarding privacy issues.¹⁷¹⁸ We, therefore, believe that similar conclusion could be easily drawn for the Spanish digital contact tracing activities as well, considering it inevitably has data processing activities, as any potential random application that was being subject to such concerns. As such, in order to elaborate on these concerns, we would like to deep dive into potential red flags that occurred during the implementation of the tool.

To begin with, as detailed in the previous section, on the positive side, there has not any been any major personal data breaches that required notification to data subjects and data protection supervisory authorities in the sense of GDPR¹⁷¹⁹ and Ley Orgánica 3/2018,¹⁷²⁰ resulted from the usage of the application in the form of data security shortages, till date. Nevertheless, there were evidently some instances, where certain security problems arose and reported by the developers of the application or users that experienced these issues during their use. The significance of privacy regarding sharing medical

¹⁷¹⁷ Kozyreva, Anastasia; Lorenz-Spreen, Philipp; Lewandowsky, Stephan; Garrett, Paul M.; Herzog, Stefan M.; Pachur, Thorsten and Hertwig, Ralph (2021) "Public perceptions of COVID-19 digital contact tracing", *op.cit.*, p.3.

¹⁷¹⁸ Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth; Camtepe, Seyit and Ranasinghe, Damith C. (2021) "An empirical assessment of global COVID-19....", *op.cit.*, p.1096.

¹⁷¹⁹ Velicia-Martin, Felix; Cabrera-Sanchez, Juan-Pedro; Gil-Cordero, Eloy and Palos-Sanchez, Pedro R. (2021) "Researching COVID-19 tracing app acceptance: incorporating theory from the technological acceptance model", *PeerJ Computer Science*, vol.7, e316, pp.1-20, p.5.

¹⁷²⁰ The EDPB provided in Guidelines 9/2022 on personal data breach notification under GDPR that Article 33(1) of the GDPR stipulates that breaches deemed improbable to endanger the rights and freedoms of individuals do not necessitate notification to the supervisory authority. For instance, if personal data is already publicly accessible and its disclosure doesn't pose a probable risk to the person, notification may not be required. This differs from the current breach notification obligations outlined in Directive 2009/136/EC for providers of publicly accessible electronic communications services, which mandate notification of all pertinent breaches to the competent authority. For the full part see Guidelines 9/2022 on personal data breach notification under GDPR, p.18.

information is undeniable,¹⁷²¹ and the same goes for the data security automatically. Therefore, our aim is to delineate those reported or spotted vulnerabilities, and explain and address what sort of responses were provided or could have been provided from data protection law perspective, considering the future case scenarios.

The first data protection and security related concern pertaining to Radar Covid application occurred during the development of the application itself. To provide further detail thereon, even though the pilot program was carried out in June, 2020 in the island of La Gomera in the Canary Islands, citizens were only able to access the application's source code in September, 2020.¹⁷²² Accordingly, such late access to the source code inevitable raised the risk of concerns happening in the society. In more detail, INDRA, the overseeing entity for the development, established a repository for accessing the application's code, facilitating tracking of various pull requests and modifications.¹⁷²³ However, worth noting that this repository was established post the initial version's release on mobile stores, hence lacking developmental history from earlier phases.¹⁷²⁴ From the security point of view, for some, the efficacy of Radar Covid hinged upon the collective confidence vested in the application due to this incident. Thus, a pivotal initial stride toward bolstering this confidence would be the public release of its

¹⁷²¹ Velicia-Martin, Felix; Cabrera-Sanchez, Juan-Pedro; Gil-Cordero, Eloy and Palos-Sanchez, Pedro R. (2021) "Researching COVID-19 tracing app acceptance...", *op.cit.*, p.6.

¹⁷²² Carrasco, Sergio, (2021) "Failure of Radar Covid App", Liberties available at: <https://www.liberties.eu/en/stories/app-radar-covid-rights/43524> (accessed on 22 June 2024).

¹⁷²³ See Rights International Spain Report (2021) "Tracking Apps In The Eu Lessons For Future Use Of Technology In Combating Social Challenges The Spanish Case: Radar Covid Application", p.3. The document was authored by Sergio Carrasco Mayans, a consultant and specialist in data protection and privacy at Rights International Spain. This report was prepared within the scope of the European initiative "Contact tracing in the EU: Lessons to be learned for the future use of technology in fighting societal challenges," led by the Civil Liberties Union for Europe. Funding for this project was provided by the Network of European Foundations and the European AI Fund, with Rights International Spain overseeing implementation in Spain. The European AI Fund, facilitated by the Network of European Foundations (NEF), supported this project. However, it's important to note that the organizers bear full responsibility for the project, and its content may not necessarily reflect the perspectives of the European AI Fund, NEF, or their partner foundations.

¹⁷²⁴ Rights International Spain Report, (2021) "Tracking Apps In The Eu Lessons For Future Use Of Technology In Combating Social Challenges The Spanish Case: Radar Covid Application", p.4.

code.¹⁷²⁵ We certainly agree this point of view brought by Romero (H&A) as we also recommended in the previous chapters. Correspondingly, we are of view that unavailability of source code or any other key technical information that could be shared with the public review is not often the most transparent approach from data protection law perspective, and what we emphasized in previous chapters pertaining to the disclosure of DPIA by data controllers may also be leveraged for the transparent implementation of technical aspects of the applications. Nonetheless, on the positive side, for the sake of accuracy and fairness, although it was late and there were certain criticisms related to this missing part, Spanish data controller in conjunction with INDRA took the right approach and shared all necessary technical information on publicly available website, namely Github website devoted to the technical aspects of the application, which we find in the spirit of the data protection requirements in many sense.

Additionally, considering that the application launched under the Mozilla Public License 2.0., which is an open source code license, this decision aligned with the pro Open Source movement's objective of fostering collaborative development to enhance the application with open access to the source code, users could be able to identify, report, and address potential bugs, as well as introduce new features.¹⁷²⁶ In addition, as it is accessible to everyone, external programmers or auditors can also identify errors, bugs, and security vulnerabilities.¹⁷²⁷ That being said, it is still important to caveat that an open-source application enables other developers to analyze, verify, and audit the code thoroughly, particularly in the pursuit of identifying potential "0-day exploits", those lingering security vulnerabilities that remain

¹⁷²⁵ Romero, Mario, (2020) "Covid Radar, is it Safe?", H&A Group Publications available at: <https://www.hyaip.com/en/news/covid-radar-is-it-safe/> (accessed on 23 June 2024), para.6.

¹⁷²⁶ UDS Enterprise (2021) "Radar COVID app source code to be released next week" available at: <https://udsenterprise.com/en/radar-covid-app-source-code-released-next-week/> (accessed on 20 November 2023), para 1.

¹⁷²⁷ Castillejos Torregrosa, Nuria (2021) "Personal data protection and Covid-19. The eternal dilemma: Security or Liberty?", Universidad de Alicante. Departamento de Filosofía del Derecho y Derecho Internacional Privado, p.11.

unresolved.¹⁷²⁸ Nonetheless, we still are of view that this approach did definitely contributed to promote transparency, enabling individuals to independently verify whether the app developer is truthful in asserting that it does not gather any detrimental information.¹⁷²⁹ In other words, it fostered the culture of transparent processing of personal data, by supporting the technical feasibility as well, which would definitely outweigh the potential drawbacks associated with the publishing source codes, in line with what we provided above for the information campaigns of data controllers. Furthermore, we believe that by adopting this approach, the Spanish data controllers also addressed certain speculations suggesting hidden functionalities within the app or potential privacy risks for users. As also called out by Rodríguez-Prieto for inclusion of third-party companies that substantive elements of the app that remain hidden, about which experts cannot opine or audit.¹⁷³⁰ Therefore, transparency requirement in line with the GDPR principles seem to be supported with technical nuances that were carried out by the Spanish controllers, despite their delay.

Also, as one of the multiple benefits of this transparent approach within the security context, data subjects could be able to demonstrate their concerns and provide their feedback regarding the security details of the application. For instance, some users expressed concerns over technical issues and false positive notifications, which affected the app's effectiveness.¹⁷³¹ More specifically, as detailed by the study of Carrasco that, upon the release of the repository, third parties identified privacy concerns associated with the implementation of DP-3T in the app, notably the absence of false traffic when

¹⁷²⁸ Romero, Mario (2020) "Covid Radar, is it Safe?", H&A Group Publications, para 6.

¹⁷²⁹ Castillejos Torregrosa, Nuria (2021) "Personal data protection and Covid-19...", *op.cit.*, p. 11.

¹⁷³⁰ Rodríguez Prieto, Rafael (2020) "Consecuencias de la STC 76/2019, de 22 de mayo en la privacidad y uso de apps para el control de la COVID. El caso de Radar COVID", *Cuadernos electrónicos de filosofía del derecho*, vol. 43 pp.189-219, p.210.

¹⁷³¹ Kyotu Technology Report (2020) "Unveiling the impact of covid tracking apps around the globe" <https://www.kyotutechnology.com/unveiling-the-impact-of-covid-tracking-apps-around-the-globe/> (accessed on 23 June 2024).

transmitting a positive case to the servers.¹⁷³² Given that the app only communicated with the servers in case of a positive case, identifying individuals who tested positive appeared relatively straightforward.¹⁷³³ While we understand that it might be detrimental for the users identity, as it might have resulted in a circumstances, in which the user identities could have been revealed by the application, so far, almost two years later application becoming demised, we have not encountered with any personal data breach or privacy risk posed to the data subjects of this sort. On the contrary, we believe that the study of van Dijk, and colleagues have provided a meaningful contribution these discussions by analyzing the data collected by the application, not to cause any ambiguity within this context. As per their study The Covid Radar app effectively gathered anonymized, user-reported data on COVID-19 symptoms and adherence to social distancing measures.¹⁷³⁴ The research indicated that initial validation demonstrated a correlation between symptoms and behavior reported within the app and subsequent in-app reporting of a Covid test. Additionally, external validation illustrated the predictive capability of COVID Radar, as in-app reported positive COVID tests closely aligned with state-reported case counts.¹⁷³⁵ Hence, it indirectly pointed out the same direction what we recommended that it did not result in the feared events called out by the research of Carrasco. As per their research, it did not only collect anonymous data, but also implemented an efficient tracking with the anonymized personal data. As we called out earlier in this research that we cannot fully interpret the success of the application from health efficiency perspective, as it does not fall within the scope of this research, yet, it is plausible to observe that such alleged success were at least

¹⁷³² Carrasco, Sergio, (2021) "Failure of Radar Covid App", Liberties available at: <https://www.liberties.eu/en/stories/app-radar-covid-rights/43524> (accessed on 22 June 2024), para 12.

¹⁷³³ Carrasco, Sergio, (2021) "Failure of Radar Covid App", Liberties, para 13.

¹⁷³⁴ van Dijk, Willian J.; Saadah, Nicholas H.; Numans, Mattijs E.; Aardoom, Jiska J.; Bonten, Tobias N.; Brandjes, Menno; Brust, Michelle et al. (2021) "COVID RADAR app: description and validation of population surveillance of symptoms and behavior in relation to COVID-19", *Plos one* 16, no. 6 e0253566, pp.1-18, p.14.

¹⁷³⁵ van Dijk, Willian J.; Saadah, Nicholas H.; Numans, Mattijs E.; Aardoom, Jiska J.; Bonten, Tobias N.; Brandjes, Menno; Brust, Michelle et al. (2021) "COVID RADAR app:...", *op.cit.*, p.14.

could still be measures despite the most privacy-friendly approach, i.e., anonymous data, as targeted by the controllers of the app, which is satisfying from the data protection law perspective as it refrained from user identification with different channels.

Nonetheless, rather than potential exposure of user identities, there were other concerns raised by scholars. More specifically, pertaining to the potential vulnerability of DP-3T protocol employed by the application, an interesting approach was brought by the study of Martínez Martín through which they analyzed the security of the DP-3T protocol against several attacks, such as backend impersonation attack, false report attack, vulnerability of released cases and etc., that compromise users' data privacy.¹⁷³⁶ They provided that after analyzing the attacks initially proposed, they have determined that the DP-3T protocol was not secure against any of them¹⁷³⁷. Through the DP-3T tool, they discovered at least one attack trace for each of the attacks we analyzed. Or differently, as another potential security gap, study of Leith and Farrell called out the feature of Radar Covid that it did not employ SSL certificate pinning to ensure secure communication with the accurate server.¹⁷³⁸ The privacy concern arising from the absence of pinning is that user transactions within, for instance, an enterprise network utilizing features like "Android work", are at risk of exposure to the employer.¹⁷³⁹ This could potentially result in actions such as the uploading of keys following a positive test phone call being logged by the employer's network security devices, which would exacerbate potential concerns pertaining to third party access as detailed in Chapter 2. For the sake of keeping strict focus on this research, we are not able to address all of the technical details herein, as reiterated in different chapters that we are dealing

¹⁷³⁶ Martínez Martín, Daniel (2021) "Verificación automática del protocolo DP-3T asociado a las aplicaciones COVID-19", Universitat Politècnica de València, <http://hdl.handle.net/10251/173383>, p.39.

¹⁷³⁷ Martínez Martín, Daniel (2021) "Verificación automática del protocolo DP-3T...", *op.cit.*, p.39.

¹⁷³⁸ Leith, Douglas J., and Farrell, Stephen (2021) "Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps", *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, IEE, pp. 1-10, p.2.

¹⁷³⁹ Leith, Douglas J., and Farrell, Stephen (2021) "Contact tracing app privacy: What data is shared...", *op.cit.*, p.8.

with the security concerns from data protection law perspective, which obliges us to interpret technical issues from the regulatory perspective.

Nonetheless, our recommendation for avoiding this and any potential similar kind of vulnerabilities is that data controller must do perform its duties precisely to integrate both legal and technical experts prior to rolling out this application, as advised in Chapter 4. It is evident that DPIA cannot predict and reveal all and each type of technical vulnerabilities. However, establishing more general but quick intervention mechanisms with technical experts from data science and cyber security backgrounds could strictly bolster the general compliance program of controllers. As provided in Chapter 4 that establishing a regular consultancy mechanism with competent bodies such as European Union Cyber Security Agency, or Spanish Cyber Security Agencies could be a good starting point for this. Although DPIA was extensive, we have not been able to display such organizational measures comprising the collaboration of this kind. Alongside with these mechanisms, we are of view that what AEPD guidelines provided for Recommendations¹⁷⁴⁰ to protect personal data in situations of mobility and telecommuting guidance, particularly with respect to providing functional guidelines to both data subjects and its personnel and to a contact person must be identified to report any incident affecting personal data, as well as the suitable channels and formats to deliver such notification.¹⁷⁴¹

Subsequently, another heated topic that was already described above, as well as in Chapter 2 and Chapter 4 respectively, the third-party companies' involvement, which, inevitably, is one of the most remarkable concerns of data subjects in Spain as well. Considering that the app was built using secure Microsoft technologies, including Azure SQL Server, Azure Data Bricks, Azure Blob Storage, and Open Street View, along with various COVID-19 data

¹⁷⁴⁰ For the full Guideline see AEPD (2020) "Recommendations to protect personal data in situations of mobility and telecommuting guidance" <https://www.aepd.es/documento/nota-tecnica-proteger-datos-teletrabajo-en.pdf> (accessed on 15 February 2024).

¹⁷⁴¹ AEPD (2020) "Recommendations to protect personal data in situations....", *op.cit.*, p.1.

sources.¹⁷⁴² or similarly, in alignment with the DP-3T protocol, a public cloud server was utilized to manage confirmed positive identifiers and additional functionalities such as surveys. The app was coded in Kotlin for Android and Swift for iOS)¹⁷⁴³. Thus, as seen, like other European counterparts, Spanish application was also reliant on technology giant third-party companies. We are inclined to provide a similar response on this aspect of Radar Covid, by stating that although inclusion of technology companies always brings potential concern on the excessive processing activities without authorization, to be realistic, considering the era of technology, and the urgency of the situation, it was required to utilize the know-how of the technology companies to develop such application. Hence, we believe that there are certain data protection risks and potential negative outcomes, if intrusive processing activities take place, as detailed in Chapter 2, yet, it is even more important to rely on the efficient safeguards as also pointed out by the EDPB.¹⁷⁴⁴ The similar point was raised by the study of Rodríguez-Prieto that the participation of private companies that are also involved in serious accusations of abuse of dominant position or invasion of individuals' privacy makes it necessary, at the very least, to be cautious, in an app in which citizens place their trust because their political leaders tell them it can help control a pandemic that is costing thousands of lives and economic ruin to broad sectors.¹⁷⁴⁵

Nonetheless, again, till date, we have not encountered any major breach or suspicious activities of those actors. Furthermore, in any case, just to avoid the potential feared events, implementing AEPD recommendation for this specific situation could play an important role to refrain from these risks in its entirety. In more detail, AEPD advised data controllers pertaining to the covid apps and websites that private organizations working with public authorities

¹⁷⁴² Openasapp Website Article, Radar Covid App <https://openasapp.com/covid-19-radar-app/#use-it> (accessed on 15 February 2024).

¹⁷⁴³ Rodríguez-García, Jorge Pablo, Santiago Graña, Eva Elisa Álvarez-León, Manuela Battaglini, Francisco Javier Darías, Miguel A. Hernán, Raquel López et al. (2021) "A population-based controlled experiment assessing the epidemiological impact of digital contact tracing", p.2.

¹⁷⁴⁴ See EDPB (2020) Guidelines 04/20, *op.cit.*, p.9.

¹⁷⁴⁵ Rodríguez-Prieto, Rafael. (2020) "«Consecuencias de la STC 76/2019, ...", *op.cit.*, p.210.

may only use the information in line with their instructions and under no circumstances for reasons other than those specifically permitted.¹⁷⁴⁶ The legitimacy for data processing, therefore, would not exist, if users utilized applications or websites that are supplied by private organizations or individuals rather than by public bodies.¹⁷⁴⁷ This caveat, accordingly, aimed to prevent any feared events resulted from arbitrary acts of third-party companies, such as collecting, or storing personal data without explicit permission of data controllers and data subjects for their marketing use and etc.

Having said, while we have not observed any drastic personal data breach caused by these tech companies within unauthorized access of personal data context, there were only some relatively minor breaches appeared within the same vein. To provide more specific example on this matter, as study of Rodríguez Jurado is also dealing with this very topic, the security breach was related to data traffic.¹⁷⁴⁸ Since only positive cases were sending data to the server, anyone with access to the traffic information could identify who was sending these positive cases.¹⁷⁴⁹ Access to this information is not available to any ordinary user, but its exploitation extends beyond telecommunications and internet providers. For example, one of the tech companies might have had access to this information, as the upload to the server is done using software from the U.S. company, allowing them to identify which mobile devices were sending positive cases.¹⁷⁵⁰ Besides major companies, any individual or company with access to the same Wi-Fi network from which these codes are sent could also have access. Likewise, there were serious concerns and criticisms around traffic analysis and logs implemented by the

¹⁷⁴⁶ AEPD (2020), Notice on coronavirus self-assessment apps and website <https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites> (accessed on 7 August 2023).

¹⁷⁴⁷ AEPD (2020), Notice on coronavirus self-assessment apps and website <https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites> (accessed on 7 August 2023).

¹⁷⁴⁸ Rodríguez Jurado, Pedro (2021) "El derecho a la protección de datos y COVID19. Especial significación en el ámbito laboral." Master's thesis, published in Universidad Loyola Website, Master Universitario En Asesoría Jurídica De Empresas Tutor D^a Carmen García Ruíz), p.30.

¹⁷⁴⁹ Rodríguez Jurado, Pedro (2021)"El derecho a la protección de datos ...", *op.cit.*, p.30.

¹⁷⁵⁰ Rodríguez Jurado, Pedro (2021)"El derecho a la protección de datos ...," *op.cit.*, p.31.

application. Although this traffic was encrypted and the content of the communication was anonymous, if it is uploaded to the server, it implies that the user is positive.¹⁷⁵¹ Whoever had access to traffic, therefore, could be able to know who it was. More specifically, upon monitoring the application traffic, the reviewer identified calls to servers for which they found no justification. Specifically, one of the users have detected requests on port.¹⁷⁵² Notably, one user detected requests on a specific port. This user reported that despite having the "energy saving" option disabled, the app incorrectly informed them that it was not functioning due to this setting.¹⁷⁵³ Nevertheless, the user noted that the app remained usable across various versions of Apple and Android.¹⁷⁵⁴ On the issue of unauthorized access to logs, the findings from Appcensus, a privacy-focused company, suggest a risk of permitting phone hardware manufacturers, network operators, and their commercial associates (such as advertising libraries) to pre-install "privileged" apps, which could compromise user privacy.¹⁷⁵⁵ One feature of these privileged apps was that they have access to additional permissions that are otherwise not afforded to third-party apps downloaded.¹⁷⁵⁶ Therefore, it raised concerns in the eyes of users and scholars as well. Having said that the research concluded that it was unlikely that they collect log data with the understanding that they are now receiving user's medical and other sensitive information because of such implementation. Therefore, from our perspective, as also called out for the aforementioned concern, it is very much important to observe that the

¹⁷⁵¹ Colome Perez, Jordi (2020) "La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento, El Pais, <https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html> (accessed on 22 June 2024).

¹⁷⁵² Git Hub, Technical Issues No.47, Traffic analysis: strange calls to URLs available at: <https://github.com/RadarCOVID/radar-covid-android/issues/47> (accessed on 23 December 2023).

¹⁷⁵³ Git Hub, Technical Issues No.12, Energy saving issue, available at: <https://github.com/RadarCOVID/radar-covid-android/issues/47> (accessed on 23 December 2023).

¹⁷⁵⁴ Git Hub, Technical Issues No. 48, Lower required android version, available at: <https://github.com/RadarCOVID/radar-covid-android/issues/47> (accessed on 23 December 2023).

¹⁷⁵⁵ Joel Reardon, (2021) "Why Google Should Stop Logging Contact-Tracing Data?", AppCensus Publication, <https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/> (accessed on 23 June 2024), para 7.

¹⁷⁵⁶ *Ibid.*

Secretary of State announced in its official account that this problem had already been solved with the latest update.¹⁷⁵⁷

In other words, the Spanish Government was compelled to introduce patches on different servers to ensure the anonymization of positive individuals by sending false positives to the server via the app to make it impossible to identify their identities in case of an attack.¹⁷⁵⁸ As a risk mitigating factor from technical and organizational measures perspective in the sense of the GDPR and Ley Orgánica 3/2018, we agree with the study that no one simply not log sensitive data to the system log in the first place. To this end, in line with our approach on solidified technical and organizational measures, and privacy-by-design with aforementioned balance, study of Montesinos Rodrigo also provided that emphasizing user non-identification is crucial due to the subject matter: health data, specifically COVID disease transmissions¹⁷⁵⁹. We are also of view that the measures such as pseudonymization, encryption, confidentiality agreements, strict distribution of access roles, and the establishment of access restrictions and records that were employed,¹⁷⁶⁰ supported the solid response to such attacks and third-party related concerns. We, thus, believe that existence of these features implemented as part of privacy-by-design approach of the Radar Covid app, as per the DPIA document and privacy policy thereof, and those patches provided by the Spanish controllers, prevented any type of more serious data breach or material impact on data subject rights to happen till date. Similar conclusion from different perspective was also discussed in the research conducted by Raman and colleagues, which analyzed various contact tracing applications from a technical standpoint, Spain received high marks, along with a select few other countries, in areas concerning privacy, transparency, data

¹⁷⁵⁷ Colome Perez, Jordi (2020) "La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento, El Pais, <https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html> (accessed on 22 June 2024).

¹⁷⁵⁸ Rodríguez Jurado, Pedro (2021) "El derecho a la protección de datos ...", *op.cit.*, p.30.

¹⁷⁵⁹ Montesinos Rodrigo, Laura. (2022) "Guía para la realización del Privacy Impact Assessment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos." PhD diss., Universitat Politècnica de València, pp. 1-72, p.53.

¹⁷⁶⁰ Montesinos Rodrigo, Laura. "Guía para la realización...", *op.cit.*, p.54.

management, and security,¹⁷⁶¹ which we find promising from the regulatory perspective, based upon the non-existence of any claim, regulatory action nor action triggered by AEPD.

In conclusion, although there are other infringements of certain data protection principles from the regulatory perspective rendered by AEPD, which will be elaborated in the following section, those issues are not related to data security aspects, but rather related to other principles of data protection law. As such, till date, almost two years later (update) after the application demised, there has not been any reportable data protection incidents¹⁷⁶², in the sense set out in the EDPB Guideline.¹⁷⁶³ On the ideal level, considering what GDPR and Ley Orgánica 3/2018 obliged data controllers to do was actually tried to be fulfilled by Spanish data controller on technical level. The reason being is that the app had Bluetooth tracing, DP-3T platform, anonymity of data subjects, auto deletion of processed data within defined periods, conceivable interface etc. on the paper, which seems pleasant for us to observe, in line with data protection law requirements. When it comes to other data protection concerns, it is understandable that lack of detailed DPIA and detailed privacy policy were factors that exacerbated the user concern, as discussed in this Chapter. Accordingly, we still must give the credit of data controller for establishing most of the key risk mitigants mentioned above by adhering to the GDPR and Ley Orgánica 3/2018 requirements, although it is not fully sufficient itself, which at least demonstrated the right behavior expected from controllers for covering the technical parts of their compliance efforts.

4. AEPD Resolutions PS/00222/2021 and PS/00223/2021

As briefly mentioned in the previous Chapter, multiple parties, including professors and investigators, lodged complaints with the AEPD against the

¹⁷⁶¹ Raman, Raghu; Achuthan, Krishnashree; Vinuesa, Ricardo and Nedungadi, Prema (2021) "COVIDTAS COVID-19 Tracing App Scale...", *op.cit.*, p.11.

¹⁷⁶² See Article 33 of the GDPR, Notification of a personal data breach to the supervisory authority.

¹⁷⁶³ See the EDPB (2022) Guidelines 9/2022 on personal data breach notification under GDPR, adopted 28 March 2023, available at: https://edpb.europa.eu/system/files/2023/04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf, p.7.

SEDIA on September 7, 2020.¹⁷⁶⁴ These complaints were made on different dates starting from May 26, 2020, and covered various aspects related to data processing, security, user privacy, and compliance with GDPR principles¹⁷⁶⁵. After these complaints, the AEPD sought comprehensive information from both SEDIA and General Secretariat of Digital Health, Information, and Innovation of the National Health System (“DGSP” or later “SGSDII”) to ensure compliance with data protection regulations concerning the handling of personal data within the Radar COVID application. In summary detail, these requests encompassed a wide range of aspects including whether the Radar Covid application complies with the principles set out under the GDPR and Ley Orgánica 3/2018, in accordance with the EDPB guidelines, and following sanctions were rendered by the AEPD for SEDIA and DGSP, and classified as serious and very serious.¹⁷⁶⁶ We, therefore, find it useful to delineate the consequence of the decisions rendered by AEPD against both SEDIA and DGSP at one instance, as Rubi Puig and Herrerias Castro provided in their studies.¹⁷⁶⁷

For both SEDIA and DGSP:

- Article 5.1.a of the GDPR¹⁷⁶⁸: Breach of the principle of lawfulness, fairness, and transparency in the processing of personal data. (Very serious - Article 83.5.a of the GDPR)
- Article 5.2 of the GDPR¹⁷⁶⁹: Breach of the obligation of proactive responsibility. (Very serious - Article 83.5.a GDPR)
- Article 12 of the GDPR¹⁷⁷⁰: Failure to provide information in a concise, transparent, intelligible, and easily accessible manner,

¹⁷⁶⁴ See PS/00222/2021, Antecedents, second.

¹⁷⁶⁵ See PS/00233/2021, Antecedents, second.

¹⁷⁶⁶ See PS/00233/2021, resolución; PS/00222/2021, resolución.

¹⁷⁶⁷ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) “«COVID Radar» and protection...”, *op.cit.*, p.262-263.

¹⁷⁶⁸ As per the Article 5.1.a of the GDPR “personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”.

¹⁷⁶⁹ As per the Article 5.2 of the GDPR “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1”.

¹⁷⁷⁰ See Article 12 of the GDPR, Transparent information, communication and modalities for the exercise of the rights of the data subject.

using clear and plain language. (Very serious - Article 83.5.b GDPR)

- Article 13 of the GDPR ¹⁷⁷¹ : Failure to provide mandatory information regarding the processing of personal data. (Very serious - Article 83.5.b GDPR)
- Article 25 of the GDPR ¹⁷⁷²: Infringement of obligations derived from data protection by design, for omitting the adoption of technical and organizational measures, not conducting relevant impact assessments, and not adopting necessary guarantees in processing. (Serious - Article 83.4.a GDPR)
- Article 28.3 of the GDPR ¹⁷⁷³: Omission of the duty to have a contract or legal act regulating the relationship between the data controller and data processor (between DGSP and SEDIA, and between DGSP/SEDIA and INDRA). (Serious - Article 83.4.a GDPR)
- Article 35 of the GDPR ¹⁷⁷⁴ : Failure to produce an impact assessment before the development of personal data processing operations. (Serious - Article 83.4.a GDPR).

For DGSP specifically:

- Article 28.1 of the GDPR ¹⁷⁷⁵: Failure to select a data processor that offers sufficient guarantees to implement appropriate technical and organizational measures, ensuring compliance with GDPR requirements and safeguarding the rights of data subjects. (Serious - Article 83.4.a GDPR).

For SEDIA specifically:

¹⁷⁷¹ For the full article see Article 13 of the GDPR, Information to be provided where personal data are collected from the data subject.

¹⁷⁷² For the full article see Article 25 of the GDPR, Data protection by design and by default.

¹⁷⁷³ For the full article see Article 28.3 of the GDPR, Processor.

¹⁷⁷⁴ For the full article see Article 35 of the GDPR, Data protection impact assessment.

- Article 28.10 of the GDPR¹⁷⁷⁶: Overstepping the performance of functions as a data processor, assuming the role of data controller. (Serious - Article 83.4.a of the GDPR)

Hence, as clearly indicated above that both SEDIA and DGSP were deemed breaching the respective principles of the GDPR. Nonetheless, these sanctions were merely of a warning, without any economic penalty, rather than economic fines. Having said that, it should not underestimate the seriousness of the Government's action, as such decision was only a consequence of the fact that Ley Orgánica 3/2018 and the GDPR did not contemplate fines when non-compliance is carried out by a public administration.¹⁷⁷⁷ Correspondingly, following to this general description of both decisions, we would like to delve into the details of both decisions rendered against DGSP and SEDIA respectively to analyze and address the most remarkable aspects thereof.

To this end, first of all, we believe that the most heated topic was brought into to the AEPD was the relationship of right to data protection and state of alarm. In its allegations, the SEIDA argued that, living in a state of health alarm, the data protection rights of the interested parties should be understood in light of the state of need to develop the disease control measure, under article 3¹⁷⁷⁸ of the Civil Code.¹⁷⁷⁹ This argument has been rejected by the AEPD, which stated that the fundamental right to data protection was not suspended by the

¹⁷⁷⁷ Merino, Marcos (2022) "La app Radar COVID violó 8 artículos de la normativa de protección de datos: la AEPD acaba de sancionar al Gobierno" available at: <https://www.genbeta.com/actualidad/app-radar-covid-violo-8-articulos-normativa-proteccion-datos-aepd-acaba-sancionar-al-gobierno> (accessed on 25 December 2023).

¹⁷⁷⁸ Article 3 of the Spanish Civil Code sets out that:

"Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquéllas.

Donde hay duda acerca del sentido de una norma, ésta deberá ser interpretada en el sentido que sea más conforme con la Constitución Española y con la normativa comunitaria."

¹⁷⁷⁹ See Recurso de reposición Nº RR/00189/2022, Examinado el recurso de reposición interpuesto por SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos (en lo sucesivo, AEPD) en el procedimiento sancionador PS/00222/2021, y en base a los siguientes, general allegations, HECHOS, eighteenth section.

mere declaration of a state of alarm, but this suspension was limited to the cases of declaration of a state of emergency or siege, as established in article 55.1 of the Constitution. As such, AEPD reiterated that during the state of alarm, the exercise of rights can only be conditioned, but not suspended. In this specific case, a state of alarm was declared, which did not imply, in any case, the suspension of fundamental rights.¹⁷⁸⁰ As also provided by the study of Campillo, during the pandemic, there was a need to find a direction that would balance public health management and data governance, approaching a weighing of rights and freedoms with public obligations.¹⁷⁸¹ Suitably, AEPD made it clear that, even though it was aware of the extraordinary and emergency situation that the pandemic generated, the right to the protection of personal data cannot be an obstacle to technological advances to combat the pandemic, as such these clear breaches of the regulations continue to be grounds for sanctions.¹⁷⁸²

Accordingly, considering these developments, we believe that as provided in the previous chapter, right to data protection is one of the most significant fundamental rights, given the nature of our era that is hugely reliant to data processing activities for any type of activity. Therefore, regulators and lawmakers ought to also consider the merits of this new era, while considering the fundamental nature of the right at stake, rather than sticking to the old school methods of enlisting the type of fundamental rights and their importance. To this end, like our approach in Chapter 6, AEPD also highlighted the fact that there should be a clear balance between the technological advancement to combat the pandemic scenarios and right to data protection. Thus, from our perspective, such decision pertaining to the intrusiveness of the activities of data controllers requires case-by-case analysis for the assessment of the existing situation to establish if they can simply rely on the chaotic atmosphere caused by extraordinary situation.

¹⁷⁸⁰ See AEPD, PS/00222/2021, y en base a los siguientes, specific allegations, B1 part.

¹⁷⁸¹ Campillo, Lorena Pérez. (2023) "La Tecnología De Localización Aplicada A La Investigación Científica: El Cumplimiento Normativo En Torno A La Protección De Datos Personales." *Revista de derecho político*, vol.117, pp. 311-340, p.314.

¹⁷⁸² See AEPD, PS/00222/2021, y en base a los siguientes, specific allegations, B1 part.

Suitably, in line with our stance during the entire research, while we do agree with the view of SEDIA that right to data protection could be interpreted considering the existing developments at the time, it would still be bold to come to a conclusion as to whether right to data protection could be entirely overridden by the benefit gained from the deployment of the application.

That being said, it must be evaluated based on its societal role and balanced with other fundamental rights, in line with the principle of proportionality. This principle requires data controllers to adhere to data protection regulations at all times. Therefore, it automatically led us to essence of the second sanction imposed by AEPD pertaining to the matter on lack of DPIA before processing activities of the pilot app took place, to see if such risks to the data protection of the individuals would actually be analyzed thoroughly.¹⁷⁸³ In fact, the first version of DPIA submitted to the Agency was on September 22, 2020, by SEDIA, and the second version on October 30, 2020. However, the data processing was already underway, violating the provisions of Article 35 of the GDPR.¹⁷⁸⁴ This assertion indicates a lack of planned DPIA despite active personal data processing. To negate data processing, it was mandatory to perform at least an initial evaluation, which has not been substantiated either. Additionally, the documentation provided before the AEPD's request lacks any records highlighting the mandatory involvement and advice from the Data Protection Officer in the DPIA.

Considering that the privacy-by-design principle signifies a shift from reactivity to proactivity and a risk-based approach mandated by the GDPR, from the earliest planning stages of data processing, this principle must be considered by each data controller, and they are quite concerning from data protection

¹⁷⁸³ See PS/00222/2021, Fundamentos De Derecho, tenth part; PS/00233/2021, Fundamentos De Derecho, eleventh part.

¹⁷⁸⁴ As per the Article 25 of the GDPR, data protection by-design and by-default, considering the current advancements in technology, the associated expenses of carrying out a task, and the characteristics, extent, context, and objectives of data processing, as well as the potential risks to the rights and freedoms of individuals resulting from such processing, the entity in control should, both during the determination of the processing methods and the actual processing itself, adopt suitable technical and organizational measures. These measures, such as pseudonymization, should be devised to effectively implement data protection principles like minimizing data, and should integrate the essential safeguards into the processing. This is done to comply with the stipulations of this Regulation and safeguard the rights of individuals whose data is being processed.

law point of view. It implies that the data controller, from the moment a potential data processing activity is designed, must protect the personal data and the rights of the data subjects, not only when the actual processing occurs. These necessities were clearly expressed in the EDPB Guidelines 4/2019 regarding Article 25 Data Protection by Design and Default¹⁷⁸⁵. More specifically, in this certain case, we do not find the logic provided by controllers sufficient, particularly when we consider the nature of the notion and the direction of EDPB setting out that throughout the entire design process of processing activities, encompassing procurement, tenders, outsourcing, development, support, maintenance, testing, storage, deletion, and other stages, the controller must carefully consider and take into account the different aspects of Data Protection by Design and by Default¹⁷⁸⁶. Therefore, it signifies the importance of early understanding of the risks as well. As detailed in Chapter 4, the privacy by design principle aligns with DPIA as it serves as a tool to determine and assess the risks of processing, allowing for the implementation of suitable technical and organizational measures to prevent the materialization of identified risks. As the Article 29 Working Party outlined in its Guidelines on Data Protection Impact Assessment¹⁷⁸⁷ and determining whether processing 'is likely to result in a high risk' for the purposes of the GDPR the DPIA should be perceived as a tool to assist in decision-making regarding the processing. Suitably, performing DPIA post-data processing does not rectify the initial failure to conduct it timely and with the necessary participation, especially considering that the lack of risk assessment and implementation of suitable technical and organizational measures has already caused intangible harm to citizens' rights and freedoms, more critical when performed by a public administration entity. From our angle, such necessity is undeniable, given the nature of the unique processing activities that was implemented for the first time during the pandemic. Within the similar vein, it was also criticized by the report of Rights

¹⁷⁸⁵ See the EDPB (2019) Guidelines 4/2019 regarding Article 25 Data Protection by Design and Default, p.14.

¹⁷⁸⁶ See the EDPB (2019) Guidelines 4/2019 regarding Article 25 Data Protection by Design and Default, p.14.

¹⁷⁸⁷ See the EDPB (2021) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p.6.

International Spain that the documents remained inaccessible to the public in the repository, with neither the media, citizens, nor civil society granted access, citing potential future changes and eventual general publication.¹⁷⁸⁸ Furthermore, the revised version of the document released later did not align with the one initially available at launch, failing to specify the alterations made despite incorporating version control.¹⁷⁸⁹ It is essential to highlight that these documents, for which access was eventually provided, were not included in the publicly accessible repository. Additionally, there was no documented version control tracking the changes made, aside from alterations in version numbering. Consequently, the general public only has access to the most recent version of the document.¹⁷⁹⁰ Lastly, regarding one of the most substantial requirements stemming from the GDPR and Ley Orgánica 3/2018, AEPD provided that no documentation has been provided to the AEPD in which the mandatory advice and participation of the DPO in the DPIA are recorded.¹⁷⁹¹ We can provide the same for the unavailability of DPO details in privacy policy, as detailed in Chapter 1. It is an essential requirement to consult with DPO for DPIAs, and considering the general risk of these processing activities, it would even be more diligent to consult for other significant implementational activities as well. As such, even though we praised the level of detail in DPIA and prompt action of data controllers, we find this late deployment of DPIA, and lack of detail on updates is concerning, in line with the points raised by AEPD. Therefore, we agree with the AEPD approach that the lack of DPIA, as well as its defective, incomplete, late, or without the participation of the DPO, constitutes a breach of the principle of proactive responsibility and privacy by design, as well as the provisions of the GDPR regarding DPIA.¹⁷⁹²

¹⁷⁸⁸ Rights International Spain Report, (2021) “Tracking Apps In The EU Lessons For Future Use...”, *op.cit.*, p.5.

¹⁷⁸⁹ Rights International Spain Report, (2021) “Tracking Apps In The EU Lessons For Future Use...”, *op.cit.*, p.5.

¹⁷⁹⁰ Rights International Spain Report, (2021) “Tracking Apps In The EU Lessons For Future Use...”, *op.cit.*, p.5.

¹⁷⁹¹ See PS/00222/2021, Fundamentos De Derecho, tenth part.

¹⁷⁹² See PS/00222/2021, Fundamentos De Derecho, sixth part.

Subsequently, as another crucial matter, we are of the similar view as AEPD that there was not detailed roles and responsibilities of data controllers and processors, including but not limited to autonomous communities, SGAD, SGSDII, SEDIA and MSND, within the scope of the processing activities. We believe that, as proposed in Chapter 6 as well, it might be resulted from the complexity of Spanish legal framework pertaining to healthcare implementation. Considering that new data controllers of the Radar Covid application identified therein (i.e. Ministry of Health and Health Departments of the corresponding Autonomous Communities and Cities) as they hold passive legitimacy in this procedure. The topic of identity of the controller and processors were quite controversial as per the AEPD decisions, which we clearly understand why as well. As rightly pointed by the AEPD that in the first version of the impact assessment, dated September 2020, both the (Ministry of Health, Social Services, and Equality (Ministerio de Sanidad, Servicios Sociales e Igualdad and hereinafter MSND) and SGAD are recognized as data controllers as stated in proven fact thirty-fifth. In the second version of the impact assessment sent by the SEDIA, the DGSP, dependent on the MSND, was introduced as the data controller, and the SGAD is recognized as the data processor, as stated in proven fact thirty-fifth.¹⁷⁹³ Furthermore, even though MSND in response to the request dated December 4, 2020, informed AEPD that the Ministry of Health exercises the role of data controller through the SGSDII, and the SGAD, dependent on SEDIA, exercises the role of data processor, SEDIA deemed to be data controller by AEPD verdict.¹⁷⁹⁴

¹⁷⁹³ See PS/00233/2021, Fundamentos De Derecho, fifth part.

¹⁷⁹⁴ According to the AEPD's findings under PS/00233/2021, SEDIA was recognized as the data controller but lacked the legal authority to fulfill this role. Despite lacking the legal coverage, SEDIA acted as the data controller for the processing activities outlined, as it determined the purposes and methods of the processing, as defined in Article 4.7 of the GDPR, and presented itself as the data controller to citizens. However, SEDIA was not competent to process personal data for the intended purposes, resulting in a lack of legitimacy under Articles 6 and 9 of the GDPR. Legitimacy in processing, especially within Public Administrations, is intricately tied to the competence of the administrative body responsible, as only the competent body can dictate the means and purposes of processing. Furthermore, there was no prior delegation of competence before the Resolution of October 13, 2020, which would have authorized the exercise of competence. The MSND, through the Directorate General of Public Health, Quality, and Innovation, was the rightful data controller for the data handled by the

Accordingly, our first assessment on the matter is that implementing vast majority of the crucial tasks, i.e. publication of DPIA, being reported into by SGAD that was owner of the application as per Terms and Conditions document of Radar Covid¹⁷⁹⁵, and etc. could inevitably be understood that SEDIA was acting as controller, in line with what the EDPB provided as well. According to the EDPB Guideline, in the absence of control dictated by legal provisions, the determination of a party as a controller should be based on an evaluation of the actual circumstances surrounding the data processing.¹⁷⁹⁶ All pertinent factual details should be considered to determine whether a particular entity has a significant influence over the processing of personal data in question. The requirement for a factual assessment implies that the status of a controller does not solely derive from the nature of an entity processing data but rather from its specific activities in each context. Put differently, the status of an entity as a controller or processor must be assessed independently for each specific data processing activity, even if the entity may fulfill both roles simultaneously for different operations.¹⁷⁹⁷ Thus, we believe that what AEPD pointed out is quite an important factor to determine role of SEDIA, as they provided that the conclusion of the emergency contract with INDRA, as the data processor, without the subsequent authorization of the actual data controller required by Article 28.2 of the GDPR, shows that SEDIA acted as the data controller deciding on the means of processing.¹⁷⁹⁸ Therefore, as seen in summary, although there is an agreement between SEDIA and Controllers, it might still be prone to confusion in the eyes of individuals in society, as they are not a data protection

Radar COVID application. However, despite having the inherent competence, MSND did not fulfill this role, nor did it utilize any techniques outlined in the LRJSP, prior to the Resolution of October 13, 2020, to delegate its responsibilities to another entity (which, for these purposes, would be the data processor). These actions, or lack thereof, constitute violations as stipulated in Articles 83.4.a) and 83.5.a) of the GDPR.

¹⁷⁹⁵ See Radar Covid, Terms and Conditions, part 5, owner of the app.

¹⁷⁹⁶ See the EDPB (2021) Guidelines 07/2020 on the concepts of controller and processor in the GDPR, available at:https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, p.12.

¹⁷⁹⁷ The EDPB (2021) Guidelines 07/20, *op.cit.* p.12.

¹⁷⁹⁸ See PS/00222/2021, Fundamentos De Derecho, seventh part.

law expert, which oblige them to interpret factual context based on their understanding.

Furthermore, as the second dimension of this matter, we find what was provided by Rubi Puig and Herrerías Castro on this matter that, given the complexity of the administrative decision-making process for developing a technological tool, it is necessary to identify who - from a data protection law perspective - assumes the role of data controller, i.e., who practically determines the purposes and means of personal data processing (Article 4.7 of the GDPR).¹⁷⁹⁹ We agree with their view that the involvement of different entities could also make it challenging to identify who assumes the role of data controller.¹⁸⁰⁰ It is probably a valid statement for the amount of data controllers due to the existence of AC level and central level data controllers as well, so it might be the other cause of such ambiguity. As such, AEPD seemed to be quite concerned about the ambiguity between the roles and accountabilities of SGAD, SEDIA, and AC as well as mentioned above. As a key takeaway from this part of the decisions, going forward, it would be of a massive importance to clearly document and delineate the roles and responsibilities of each and every data controller and processors, in line with the responsibilities of data controllers¹⁸⁰¹ and processors¹⁸⁰² set out in the GDPR, or through more specific legislation devoted to healthcare and pandemics with references to data protection matters as proposed in Chapter 6 as well. Eventually, AEPD concluded that the SEDIA assumed the role of data controller without legal coverage, indicating that it was not the competent body to handle personal data. Additionally, even if formally designated as a data processor, its actions would have exceeded its scope, potentially falling under the provisions of Article 28.10 of the GDPR.¹⁸⁰³ However, this pilot version did not seem to clearly indicate all of these responsibilities among the main actors, which, we believe, that all of these actors seemed to fail in this

¹⁷⁹⁹ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "«COVID Radar» and protection...", *op.cit.*, p.262.

¹⁸⁰⁰ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "«COVID Radar» and protection...", *op.cit.*, p.262.

¹⁸⁰¹ See article 24 of the GDPR, responsibility of controller.

¹⁸⁰² See article 28 of the GDPR, processors.

¹⁸⁰³ See PS/00222/2021, Fundamentos De Derecho, seventh part.

regard as it is quite difficult to comprehend their roles and inclusion as data controller and processor to the envisaged processing activities, particularly once we interpreted the privacy policy in conjunction with «BOE» núm. 273, de 15 de Octubre de 2020¹⁸⁰⁴, which we believe the most essential components of processing activities. More interestingly, what AEPD provided was on this ambiguity and the channel used to articulate these roles and responsibilities by referring to the value of the METD's Press Releases, which the AEPD grants on page 140, press releases represent the pinnacle of transparency and accountability and are regarded as integral components of established facts for this reason. The SEDIA can only dissent from this assertion. Press releases, essentially, are straightforward notifications issued by the METD to keep citizens and the media informed about ongoing or planned activities. Their primary function is dissemination and publicity, and it would be an overstatement to claim that they elevate transparency to its utmost extent.¹⁸⁰⁵ There are more effective instruments for this purpose, provided for in regulations and described in Law 19/2013, of December 9, on transparency, access to public information, and good governance.¹⁸⁰⁶ As mentioned in Chapter 6, Although we provided our positive evaluation on the other components of the legal orders for the development of the application in Chapter 6, there seems to be a huge ambiguity in the roles and responsibilities for the implementation of the app as controller and processor. Therefore, AEPD rightly pointed out that press releases cannot be used to assign roles of Data Controller or Data Processor, as they are mere informational documents and do not attribute competencies, and it is impossible to draw such conclusions from them, which we find in line with the data processing agreements set out by European Commission.¹⁸⁰⁷ From our

¹⁸⁰⁴ See «BOE» núm. 273, de 15 de octubre de 2020, pp.8839188398, “Obligaciones de las partes con relación a la delegación de competencias prevista en la letra a) de la cláusula primera:” <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-12339>.

¹⁸⁰⁵ See PS/00222/2021, Seventeen Part.

¹⁸⁰⁶ For the full legislation on transparency see Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. «BOE» núm. 295, de 10/12/2013.

¹⁸⁰⁷ For the full details of the standard agreements, see European Commission, Standard contractual clauses for controllers and processors in the EU/EEA, available at: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en (accessed on 4 January 2023).

perspective, instead of augmenting the discussion around the ambiguity of roles and responsibilities between controller to controller and controller to processors, what we would like to focus on is the potential remediation of these unclear aspects of the processing activities, which we find extremely crucial to address. We are of view that it starts from the moment when legislative order is passed and published, given that identity of controllers and potential parties are involved in the process is first delineated in this legal document. Such diligent approach would also require a detailed collaboration between the regulators, data protection authorities and envisaged data controllers and processors, not to skip any of their identities. This would be accompanied with devoted specific regulations as mentioned, and standard legal clauses, and draft of which are not that much time consuming, given that European Commission¹⁸⁰⁸ has plenty of drafts available.

In addition, the ambiguity in the identity of controllers and processors would cause a plenty of other confusions within the realm of data subject rights as briefly touched above. The AEPD determined and addressed vast majority of them in a meticulous manner, which we find positive for the prevention of the realm of right to data protection and privacy during the pandemic. To provide further details thereon, pursuant to the AEPD resolutions, the initial pilot version available for user download did not meet the information requirements outlined in Articles 12 and 13 of the GDPR for data subjects' rights.¹⁸⁰⁹ As data subjects could not identify who the data controllers and processors were, and the information within which did not provide a "concise, transparent, intelligible, and easily accessible" format, there could have been inevitable confusions in the eyes of data subjects. In addition to this factor entailing confusions, SEDIA denied the rights of the individuals envisaged in articles 15 to 22 of the GDPR¹⁸¹⁰, as they considered that no personal data processing was occurring, as they also defended before the AEPD.¹⁸¹¹ Ultimately, as

¹⁸⁰⁸ See the European Commission, standard contractual clauses for controllers and processors in the EU/EEA

¹⁸⁰⁹ See PS/00222/2021, Fundamentos De Derecho, ninth part.

¹⁸¹⁰ Articles 15 to 22 of the GDPR are regulating the each of data subject rights that could be implemented by data subjects against data controllers for the respective processing activity on their personal data.

¹⁸¹¹ Recurso de reposición Nº RR/00189/2022.

provided by the AEPD that since the application promoters did not acknowledge any personal data processing, they disregarded the obligations stipulated in the GDPR and other applicable regulations, resulting in a very serious violation under Article 83.5.b) of the GDPR, as we provided in Chapter 3, 4 and 5, that honoring data subject requests is one of the most crucial part of data protection law compliance. To this end, any denial of the fact that processing personal data took place would result in serious risks to the rights and freedoms of data subjects, almost as drastic as the risks generated within the context of the personal data breaches.¹⁸¹² As such AEPD concluded that it should be emphasized that initially, no information regarding the data controller, recipients, or the rights of Articles 15 to 22 was included. However, right now, the possible thing is that controllers updated privacy policy in a way that allowed the submission of data subject requests under the Articles 15 to 22 via forms,¹⁸¹³ which provides the compliance with the GDPR and Ley Orgánica 3/2018 requirements.

Therefore, such discussion on the existence of processing activities led us to consider other significant point that were subject to AEPD criticism is that data controllers were expected to assess whether the application actually processed personal data, to what extent, and from what moment. The background of this discussion is that, the investigated parties in the sanctioning procedure claimed that during the initial development phases, there was no processing of personal data as these were fictitious, and if so, the personal data had been anonymized to prevent the identification of users of the application.¹⁸¹⁴ They mentioned that initial App version (pilot) aimed to check usability, privacy perception, and solution efficacy in a simulated

¹⁸¹² The EDPB Guidelines 9/2022 on personal data breach notification under GDPR clarified the cases where notification is required for breaches. It used the term of “likely to result in a high risk to the rights and freedoms of natural persons”, similar as the article ... of the GDPR. We used the similar criteria for indicating the level of seriousness for not providing data subject rights.

¹⁸¹³ See Radar Covid Privacy Policy, part 9: What are your rights and how can you control your data?

¹⁸¹⁴ Recurso de reposición N° RR/00189/2022, Examinado el recurso de reposición interpuesto por SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00222/2021, y en base a los siguientes, part B.5, Respecto a las condiciones de uso y política de privacidad.

environment, so no health data of the pilot's participants were handled at any point.¹⁸¹⁵ For the AEPD, the application's operation during its testing phase involved storage and communication operations of various data classified as personal. As such, from the moment a user downloaded the application from available sources, there was processing of personal data. The processing of personal data began during the pilot phase when any individual could download the application, irrespective of whether manipulated data were used to test the correct functioning of the IT tool.¹⁸¹⁶ We believe that the same amount of diligence and privacy-friendly approach must be put in place from the very beginning of any type of application that is reliant on personal data processing activities, even if it employs anonymization or pseudonymization techniques during its implementation. The reason of our approach is that the risk of identification of data subjects resulted from processing personal data by any application could be reduced or vastly mitigated by technical measures, as detailed above, to some extent. Nonetheless, it does not mean that personal data processing does not take place just because such risk mitigants are employed by data controllers. Additionally, there might be other processing activities that are not directly related to the core activities of the application or data controller. For instance, as also provided by Duarte that when the primary functions do not involve data processing, any data processing activities should be deemed as ancillary.¹⁸¹⁷ More specifically, consider an e-commerce platform solely utilizing customer data to facilitate order processing and fulfillment. Here, the handling of customer data serves as a supporting function to the core activity of selling products.¹⁸¹⁸ To this end, as rightly indicated by AEPD that despite not allowing direct identification of the user or their device, the data processed did enable indirect identification. This processing included aggregated information from users of the

¹⁸¹⁵ Recurso de reposición Nº RR/00189/2022, part B.5, Respecto a las condiciones de uso y política de privacidad.

¹⁸¹⁶ See PS/00233/2021, Fundamentos De Derecho, fourth part; PS/00222/2021, Fundamentos De Derecho, fifth part.

¹⁸¹⁷ Duarte, Diogo (2019) Art. 37 GDPR: Which are the "Core Activities" of the entities? Available at: <https://www.linkedin.com/pulse/art-37-gdpr-which-core-activities-entities-diogo-duarte> (accessed on 5 March 2024), para 5.

¹⁸¹⁸ Duarte, Diogo (2019) Art. 37 GDPR: Which are the "Core Activities" of the entities? para 5.

application, both those who downloaded it and those who acted as positive cases or received risk alert notifications.¹⁸¹⁹ Correspondingly, we understand that the first scenario might not be the case for Spanish data controllers, so their reasoning is not entirely wrong. However, as rightly indicated by AEPD, the latter scenario is still viable and applicable, namely communication data of users, and their other potential personal data used for pilot phase. Thus, the same logic also applies to this specific case that there is a personal data processing activities starting from the pilot phase, which we also believe the case for Spanish controllers given that their pilot required user download of the application, which entailed so-called secondary type of processing, resulting in processing anyway.

Furthermore, within the same vein what we provided above under security issues section, AEPD pointed out the fact that the application's operation allowed for a link between an IP address and the fact that its owner was uploading a positive Covid test. The system associated the IP address with the TEK keys uploaded by users who had tested positive. The IP addresses of Radar Covid users associated with a positive COVID test could be observed by third party tech company, which provided the CloudFront CDN endpoint technology used for TEK key downloads. Thus, the application's functioning allowed unequivocally linking an IP to the fact that its owner is uploading a positive COVID test. Therefore, without the user's awareness, the app could enable third parties to know that the holder of an IP is infected by the virus, implying the communication of sensitive data, as it concerns health information. While the treatment of the IP address was necessary for the application's operation, the possibility of associating the IP with the upload of a positive test was not.¹⁸²⁰ Also, we agree with the reasoning of the AEPD that IP address should be considered as personal data, as AEPD provided that Judgment of the Administrative Litigation Chamber of the National Court of September 1, 2011 (rec. 625/2009), which establishes that the IP address is

¹⁸¹⁹ See PS/00233/2021, Fundamentos de Derecho, fourth part; PS/00222/2021, Fundamentos de Derecho, fifth part.

¹⁸²⁰ See PS/00222/2021, Fundamentos de Derecho, eight part; see PS/00233/2021, Fundamentos de Derecho, sixth part.

personal data, understanding that "the criterion of identifiability is basic to understand that the IP address must be considered as personal data and, therefore, it is subject to the same guarantees as those provided for any kind of personal data in relation to its processing [...] Applying these criteria, we must conclude that what the appellant intends regarding the IP addresses of users of P2P networks clearly falls within the concept of data processing and will therefore require the application of the criteria and general requirements of the concept of data processing.¹⁸²¹ Ultimately, health data became linked to an IP address, which, in addition to being personal data, indirectly allowed the identification of the diagnosed person, which we also agree that IP address creates vulnerability, given that it might be even used to determine the users location, similar to their use in cookies context, therefore, it should qualify as personal data as provided by the GDPR as well.¹⁸²²

Suitably, AEPD, by using the powers conferred by Article 58.1 of the GDPR and Article 67 of Ley Orgánica 3/2018, requested that within ten business days, it would be informed if data controllers are aware of this fact and, if so, the measures taken to resolve it.¹⁸²³ From our angle, it aimed to foster this swift remediation provided by data controllers, which was detailed in the previous section of this chapter. Despite the application development team's awareness of this protocol vulnerability, they deemed the risks minimal and chose not to implement any corrective measures, even when feasible. However, the issue was not addressed until October 8, 2020, nearly two months after its deployment. Consequently, the AEPD concluded that the application's design did not effectively consider the principles applicable to data protection and that in the implementation of technical and organizational security measures, the controller did not consider the risks posed by this

¹⁸²¹ See PS/00233/2021, Fundamentos de Derecho, fourth part; see PS/00222/2021, Fundamentos de Derecho, fifth part.

¹⁸²² As per Recital 30 of the GDPR, "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

¹⁸²³ See PS/00222/2021, Antecedentes, sixth part.

processing.¹⁸²⁴ In fact, according to the AEPD, even when aware of the risk, they did not integrate the necessary guarantees to ensure data confidentiality and system resilience. While both controllers, in AEPD, definitions, gradually corrected different deficiencies and adapted their behaviors to GDPR requirements, their initial actions were surprising, especially when most information was easily accessible.¹⁸²⁵ Accordingly, we agree with AEPD's perspective that, the controller has not considered the risks posed by this processing, even though they were aware of such risks.¹⁸²⁶ In more detail, AEPD provided that while the treatment of the IP address was necessary for the application's operation, the possibility of associating the IP with the upload of a positive test was not.¹⁸²⁷ Considering the DPIA and the privacy policy of Radar Covid itself, we also reached the similar conclusion. It might be signal of inaccurate rating assigned to the risks posed by the usage of IP address, rather than negligence. Regardless of the motive, it would end up in breach of both article 32 and 83 of the GDPR, pertaining to the technical and organizational measures and DPIA. Our view on this approach brought by AEPD is that they are rightly pointing this gap, as part of their duties, which is genuinely important for the society. On the other hand, from data controller perspective, it might be understandable that applications that must be deployed within a short timeframe could be prone to security issues, and that might be lack of extremely detailed risk assessments contrary to other applications that are being rolled on non-pandemic scenarios. SGAD provided in its defense that no system is entirely secure, and the decision was made to continue as halting the use and development of the app during a state of emergency for public health would pose significant risks.¹⁸²⁸ Although we do

¹⁸²⁴ See PS/00233/2021, Fundamentos de Derecho, eight part; See PS/00222/2021, Fundamentos de Derecho, sixth part.

¹⁸²⁵ Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "«COVID Radar» and protection....." op.cit., p.275.

¹⁸²⁶ See PS/00233/2021, Fundamentos De Derecho, eight part; see PS/00222/2021, Fundamentos De Derecho, sixth part.

¹⁸²⁷ See PS/00233/2021, Fundamentos De Derecho, eight part; see PS/00222/2021, Fundamentos De Derecho, sixth part.

¹⁸²⁸ Recurso de reposición N° RR/00189/2022, Examinado el recurso de reposición interpuesto por SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00222/2021, y en base a los siguientes.

not entirely exclude this truth, we also need to remind that data controllers, particularly considering that they are public institutions in this pandemic case in Spain, they should be more risk averse, which means that even if the risk is minimal, they should be able to establish risk mitigation plans in their pocket, so that it would not take months to fix or tackle any type of data security issues. Again, this leads us to the sufficiency of DPIA. Nonetheless, to be fair, in DPIA, Spanish data controllers implemented an elaborate approach, as called out earlier. For instance, the DPIA articulated that all of these random codes generated in the backend of the system and provided to the Autonomous Communities through a web service, was hosted on technology company's servers.¹⁸²⁹ Or similarly, DPIA indicated that it was necessary to collect all codes received from other users and send them to the central server for retrieval by health authorities, and it specified each of the recipients, namely health Authorities, Users and Central Positive Validation Service provided by the Administration.¹⁸³⁰ Therefore, as seen controllers were meticulous for drafting the DPIA. However, more interestingly, SGAD provided that the pilot application of the app used simulated data, as such, although the DPIA was conducted after the pilot's deployment,¹⁸³¹ it was conducted before the application handled user health data, which was also detailed above for personal identifiable data matter in this section. However, we do not agree with the reasoning that DPIA was deployed before using actual personal data, because as described below, processing activities did actually start from the pilot. First, within the same DPIA, they already mentioned that any proximity tracking system that verifies a public database of diagnosis keys against changing proximity identifiers (Rolling Proximity Identifiers - RPID) on a user's device leaves open the possibility that contacts of an infected person discover which of the people they encountered is infected. Additionally, the fact that infected users publicly share their diagnosis keys once a day, rather than their RPID every few minutes, exposes those

¹⁸²⁹ See "Informe de Evaluación de Impacto relativa a la Protección de Datos...", *op.cit.*, 2.3.4 Análisis del tratamiento, p.13.

¹⁸³⁰ See "Informe de Evaluación de Impacto relativa a la Protección de Datos...", *op.cit.*, 2.3.4 Análisis del tratamiento, p.13.

¹⁸³¹ See PS/00222/2021, Fundamentos De Derecho, sixth part.

individuals to linkage attacks. Special attention must therefore be paid to this probability, as in the event that a user of the application could be identified, privacy would be greatly threatened, potentially affecting many types of personal data such as email, call records, SMS and instant messaging, health data and etc.¹⁸³² Therefore, we found AEPD's point more viable with regard to the necessity of DPIA prior to processing activities, but it is still positive to observe that the controllers published the DPIA even with some delay, as mentioned above, which is in line with EDPB guideline that sets out that the aim of such a procedure would be to cultivate trust in the controller's handling of data, showcasing accountability and transparency.¹⁸³³ It is considered best practice to draft a DPIA publicly available when the processing operation affects members of the public. This is especially pertinent when a public authority conducts a DPIA.¹⁸³⁴

Lastly, we would like to touch base on the amount and severity of fines imposed by the AEPD on DGSP and SEDIA, as elaborated in the introduction of this section. As per the discussions taking place at the time of this decisions being rendered, there were some criticisms about the severity of the fines imposed by the AEPD. While we can understand the logic behind such reactions, considering the aforementioned criticisms, and other potential side effects that resulted from the use of the applications in other countries as well, it is important to clarify that AEPD is surely bound by the limits of GDPR and Ley Orgánica 3/2018 in this regard. Therefore, AEPD clearly explained the logic of such decisions by providing that these infringements done by accused parties were categorized under articles 83.5.a), 83.5.b), and 83.4.a) of the GDPR and classified, solely for the purpose of determining prescription periods, under articles 72.1.a), 72.1.h), and 73.d), k), m), and t) of the L.O 3/2018. Article 83.5.a) and b) of the GDPR states: "Infringements of the following provisions shall be subject to administrative fines up to 20,000,000 EUR or, in the case of an undertaking, up to 4 % of the total worldwide annual

¹⁸³² See "Informe de Evaluación de Impacto relativa a la Protección de Datos...", *op.cit.*, 2.3.2 Datos personales objeto del tratamiento, p.10.

¹⁸³³ See the EDPB (2021) Guidelines on Data Protection Impact Assessment (DPIA), *op.cit.*, p.18.

¹⁸³⁴ See the EDPB (2021) Guidelines on Data Protection Impact Assessment (DPIA), *op.cit.*, p.18.

turnover of the preceding financial year, whichever is higher.¹⁸³⁵ In addition to this, for the purpose of the prescription period, Article 72 of the the L.O 3/2018 indicates: "Article 72. Considered very serious infringements. Additionally, Article 83.7 of the GDPR states: "Without prejudice to corrective powers of supervisory authorities pursuant to Article 58(2), each member state may establish rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that member state."

In this regard, the Article 77 of L.O 3/2018, under the title "Applicable Regime to Certain Categories of Controllers or Processors," establishes the following: "1. The regime established in this article shall apply to the processing for which those responsible or processors are responsible: (...) c) The General State Administration, the Autonomous Communities Administrations, and entities within the Local Administration. (...) ¹⁸³⁶ Therefore, when the controllers or processors listed above committed any of the infringements referred to in Articles 72 to 74 of L.O 3/2018, the data protection authority competent shall issue a resolution sanctioning them with a warning.¹⁸³⁷ The resolution shall also establish the measures to be taken to cease the conduct or correct the effects of the infringement committed. The resolution shall be notified to the responsible or processor, to the hierarchically dependent body, if applicable, and to the affected parties who have the status of interested

¹⁸³⁵ See PS/00222/2021, Conclusion part.

¹⁸³⁶ For the relevant part see the full Article 77.1 of L.O 3/2018, set out that "El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas."

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales. "

¹⁸³⁷ See PS/00222/2021, Fundamentos de Derecho, Conclusion part.

parties, if applicable. As such, AEPD concluded that the L.O 3/2018 does not authorize the imposition of administrative fines but rather issues a warning, without any economic effect.¹⁸³⁸ In other words, consequently, since there was no specific sanction provided for public entities in this case, it was decided to issue a warning to the entity, in accordance with the provisions of Article 58(2)(b) of the GDPR.¹⁸³⁹

Accordingly, our view on the topic is that it is required, for sure, to follow the direction stipulated in the respective regulation, namely L.O 3/2018. However, it also obliged us to think about the essence of this sanction regime set out for the public authorities. We do believe that it is not simply logical to conclude that economic sanctions do not really fit with the spirit of activities undertaken by public institution, as they are not undertaking any economic activity. Technically, it is correct, for sure. On the other hand, as detailed in chapter 2 that commercial companies are not the only potential suspected parties of such feared events. Those events, i.e., monitoring, tracking and etc., could also be implemented by public authorities, even though they would not aim to do so. Therefore, to protect both sides, sanction regime of L.O 3/2018 should be more compelling and stricter for the situations where sensitive personal data of users might be directly or indirectly impacted. Such stricter regime does not have to be in the form of economic sanctions, but at least, further emphasize could be put on the accountability and responsibility of parties engaged with such processing activities. We believe that there should be a clear balance between the public benefit and such stricter mechanisms. However, considering the elaborate reasoning of AEPD on the pilot project, there seems to be an inconsistency between the severity of the sanction and reasons that caused the investigation at the first place. In other words, if there are such intrusive actions in terms of privacy resulted from the processing

¹⁸³⁸ See PS/00222/2021, Fundamentos de Derecho, Conclusion part.

¹⁸³⁹ See Zegarra&Schipper Abogados Publication, (2022) "Consultores Agencia Española De Protección De Datos Confirma Sanción A Entidad Estatal Por Vulnerar Las Normas De Protección De Datos Mediante Aplicación Móvil (App) Contra La Covid-19" available at <https://www.zysabogados.pe/wp-content/uploads/2022/06/004.pdf>, p.2.

activities, they might also be followed by stricter corrective plans coerced by AEPD.

That being said, what we found positive about the entire process is that as we also highlighted above for different parts of processing activities, Spanish data controllers and processors, at least, acted responsibly to remediate any potential concern that raised by AEPD, activists and public opinion, by updating their privacy policies, DPIA, and publishing their source codes, as detailed above, other than failing in clearly establishing the role and identity of controllers and processors. Hence, it also indicated that there is a good understanding of data protection law requirements, and responsibility and willingness to protect individuals from any type of privacy intrusive actions, which is definitely in line with the spirit of the GDPR perspective. Thus, to conclude the discussions, further emphasize is required on the accountability and responsibility from the legislative perspective, but overall efforts of Spanish did not fail as claimed, and actually established a good sample of privacy-first approach in multiple instances.

5. Lessons-learned for future Contact Tracing Applications in Spain and Conclusions

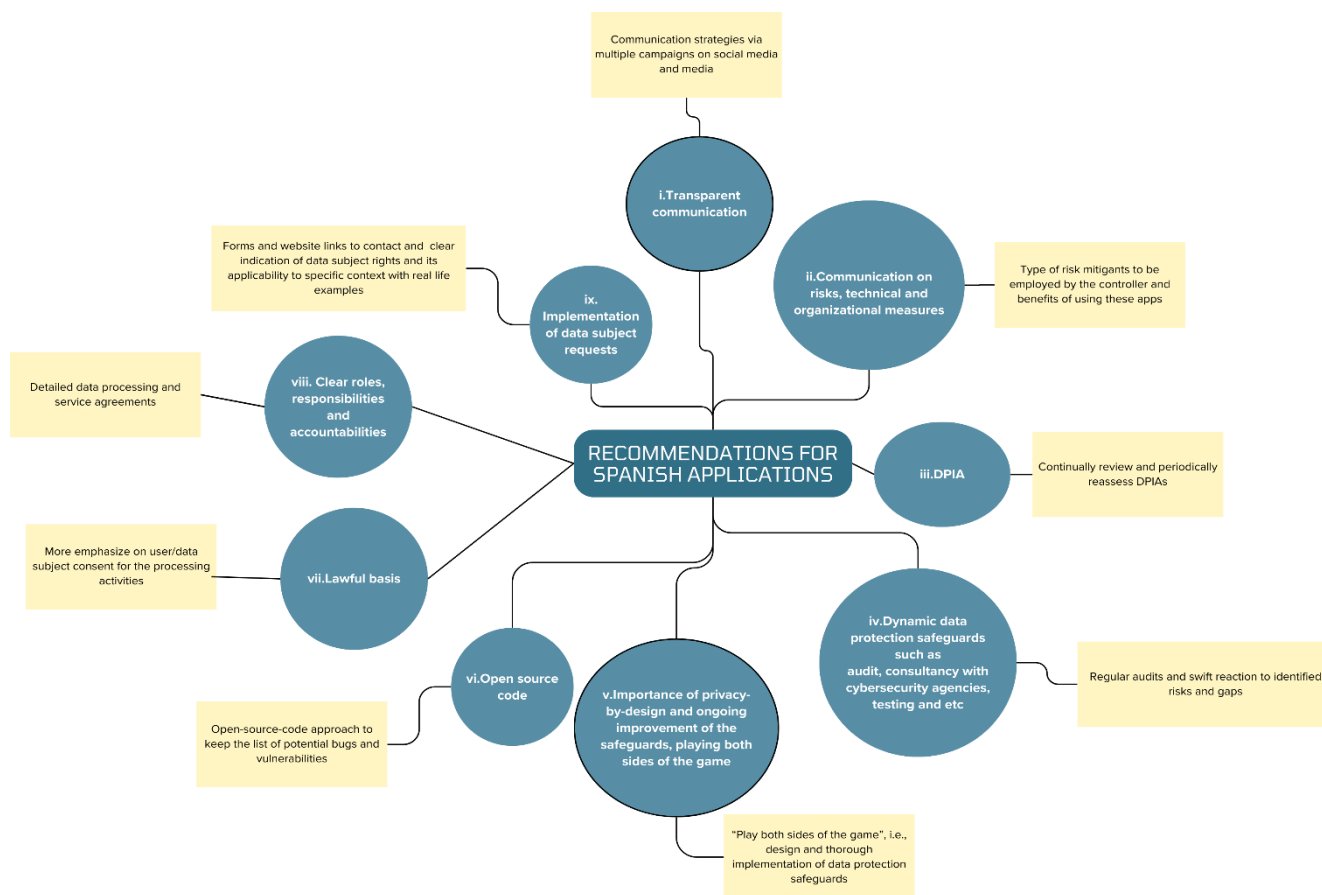
In the final section of this Chapter, we will first provide a pinpoint of what are the lessons learned for Spanish data controllers for any potential future use of these applications, in light of security issues faced by users and controllers till our date, and of concerns raised by AEPD decisions, and provide tailor made recommendations as we did in Chapter 3, 4 and 5 for other European applications, which will also be summarized via diagram for the ease of reference. By doing this, we are aiming to pinpoint the potential enhancements for the future use to implement more privacy-friendly digital contact tracing. Subsequently, we will provide our thesis statement and conclusive remarks for the entirety of the thesis as a result of this research and provide our closure for the ongoing discussions and recommendations provided.

5.1 Lessons-learned for future contact tracing applications in Spain and Concrete Recommendations

Privacy concerns and the societal implications of technology have exerted a significant influence on the acceptance and efficacy of these applications,¹⁸⁴⁰ and privacy concerns and data security emerged as primary challenges, as detailed in the entirety of this thesis, which is, no surprise, is a valid statement for Spain as well, given that Spain is one of the lowest download proportion across the EU with 18% as per the EU Commission data.¹⁸⁴¹ Therefore, as reiterated that balancing the need for effective contact tracing with safeguarding personal data remained a critical issue within Spanish jurisdiction too. We have accordingly provided below our lessons-learned for future contact tracing applications that could be utilized in Spain.

¹⁸⁴⁰ Kyotu Technology Report (2020) “Unveiling the impact of covid tracking apps around the globe” <https://www.kyotutechnology.com/unveiling-the-impact-of-covid-tracking-apps-around-the-globe/> (accessed on 23 June 2024).

¹⁸⁴¹ European Commission (2022) “Digital Contact Tracing Study on lessons learned, best practices...”, *op.cit.*, p.69.



- i. First of all, we are of the view that future iterations must indicated how it addresses privacy concerns, improve usability, and integrate seamlessly into broader public health strategies. Valuable insights gained from the deployment of contact-tracing apps underscore the pivotal role of transparent and lucid communication and public confidence in achieving widespread acceptance, which is reiterated by EDPB¹⁸⁴² and AEPD Guidelines¹⁸⁴³, as well as Transparency laws¹⁸⁴⁴ for other processing activities, which, we believe, can be leveraged to the future use of contact tracing applications in Spain, as detailed

¹⁸⁴² As stated in the EDPB (2018) Guidelines on transparency under Regulation 2016/679, transparency is about fostering confidence in the procedures that impact citizens by empowering them to comprehend and, if needed, question those procedures.

¹⁸⁴³ See AEPD, Guía para el cumplimiento del deber de informar <https://www.aepd.es/documento/guia-modelo-clausula-informativa.pdf>. (accessed on 23 June 2024).

¹⁸⁴⁴ Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. «BOE» núm. 295, de 10/12/2013.

above. To the same end, some countries, such as Poland and New Zealand, have implemented robust communication strategies to address public apprehensions, stressing the voluntary nature of app usage and its advantageous impact on public health.¹⁸⁴⁵ Therefore, the similar approach pertaining to implementation of comprehensive communication strategies via multiple campaigns on social media and media should definitely be implemented by Spanish data controllers in the future to mitigate these concerns mentioned. In other words, end-users need to be made aware of the possible hazards associated with using the app and sharing their data further.¹⁸⁴⁶

- ii. That being said, it is not merely sufficient to provide the details of envisaged processing activities. Rather, such communication and information campaigns should ideally include the level of technical and organizational measures, and other potential risk mitigants. In other words, as reiterated that the type of risk mitigants to be employed by the controller to keep controls these risks in a reasonable level must be clearly and specifically communicated to the data subject users, by adhering to the privacy notices requirements set out by the EDPB.¹⁸⁴⁷ In addition to this, benefits of implementing such applications could be clearly and understandably indicated to the users, which would lead to higher acceptance rates, more efficient contact tracing activities,

¹⁸⁴⁵ Kyotu Technology Report (2020) "Unveiling the impact of covid tracking apps around the globe" <https://www.kyotutechnology.com/unveiling-the-impact-of-covid-tracking-apps-around-the-globe/> (accessed on 23 June 2024).

¹⁸⁴⁶ Welsh, Thomas; Rekanar, Kaavya; Abbas, Manzar; Chochlov, Muslim; Fitzgerald, Brian; Glynn, Liam; Johnson, Kevin et al. (2020) "Towards a taxonomy for evaluating societal concerns of contact tracing apps", *2020 7th International Conference on Behavioural and Social Computing (BESC)*, IEEE, pp. 1-6, p.3.

¹⁸⁴⁷ As per the EDPB (2018) Guidelines on transparency under Regulation 2016/679, "the transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle: • before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained; • throughout the whole processing period, i.e. when communicating with data subjects about their rights; and • at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.", for the full description see p.5.

thereby tackling the virus more efficiently, and most importantly more privacy-friendly approach in the eyes of Spaniards.

- iii. However, challenges pertaining to accomplishment of fully compliant applications are not limited to transparency matters. Insufficient public awareness and comprehension regarding the app's operations and privacy safeguards have impeded adoption in several countries. In order to overcome this, data controllers must also focus various points. In more detail, determination of any potential vulnerabilities in terms of data protection law via elaborate and swift DPIAs in line with the EDPB guidelines.¹⁸⁴⁸ By this, before any speculation takes place, data controllers could be able to respond them with a solid confidence and accurate information. The underlying reason is it is natural that almost all data processing activities have some level of data protection law related risks given that each application is fed by certain volume of data to perform its goals. As such, the most important thing is to determine these risks efficiently using DPIAs, as also reiterated by AEPD decisions on the applications,¹⁸⁴⁹ and develop technical and organizational measures to keep these risks into the reasonable level, in line with the relevant articles of the GDPR¹⁸⁵⁰ and Ley Orgánica 3/2018¹⁸⁵¹. In other words, as we supported across this research that there are also levels of risks that are resulted from new developments, which are also pointed out by the EDPB¹⁸⁵² for updating the existing DPIA of various type of processing activities, which we definitely find crucial to act in line with the novelties introduced by our era. According to the EDPB, specific changes in data processing operations, such as removing automated decision-making or discontinuing systematic monitoring activities, can potentially reduce associated risks, possibly rendering a DPIA unnecessary. As a matter of good practice and main

¹⁸⁴⁸ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01.

¹⁸⁴⁹ See AEPD PS/00222/2021, already mentioned.

¹⁸⁵⁰ See Article 32 of the GDPR, already mentioned.

¹⁸⁵¹ See Article 32 of the Ley Orgánica 3/2018, already mentioned.

¹⁸⁵² Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, p.14.

takeaway, it is recommended to continually review and periodically reassess DPIAs.¹⁸⁵³ Therefore, even if a DPIA is not required on the certain date, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.¹⁸⁵⁴ Data controllers in Spain must interpret this situation very diligently.

- iv. In addition, aforementioned developments pertaining to the application that were both raised by public and AEPD should also oblige data controllers to consider dynamic solutions, as detailed in Chapter 4, such as consultation with cybersecurity agencies of the EU and Spain or establishing independent oversight mechanisms to monitor digital contact tracing activities and ensure compliance with privacy principles. We believe that what also provided by the study of Garousi and Cutting as lessons learnt for three of the UK applications is also applicable to Spanish applications and all applications probably, given that some apps, such as those for exposure notification, exhibit seemingly minor usability problems¹⁸⁵⁵. This brings up concerns about insufficient testing for usability and the potential for rushed releases.¹⁸⁵⁶ To this end, in order for data controllers in Spain to better position against these rushed deployment of the applications due to unexpected nature of pandemics, it is also important to conduct regular audits and reviews of digital contact tracing systems to identify any privacy risks, technical deficiencies or vulnerabilities and take appropriate measures to address them, so that data controllers can react any type of gap or change swiftly, as we both criticized and praised respectively above. In other words, technically, leveraging what was learned for these gaps observed for covid digital contact

¹⁸⁵³ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, p.14.

¹⁸⁵⁴ *Ibid.*

¹⁸⁵⁵ Garousi, Vahid, and Cutting, David (2021) "What do users think of the UK's three COVID-19 contact tracing apps? A comparative analysis", *BMJ Health & Care Informatics*, vol.28, no. 1, pp. 1-7, p.5.

¹⁸⁵⁶ Garousi, Vahid, and Cutting, David (2021) "What do users think...", *op.cit.*, p.5.

tracing activities will solidify privacy-by-design and privacy-by-default approach of controllers for sure.

- v. As such, in summary, it is important to play both sides of the game, namely design and thorough implementation of the processing activities. Both parts, in line with the recommendations we provided through the chapters, are equally important for Spanish data controllers as well, due to the called-out importance of early reactions following to the privacy mistakes made in the pilot project. Therefore, it is of massive significance to maintain the pilot projects, and leverage lessons learnt both from COVID-19 pandemic, and potential usage of pilot project to be implemented, to align with the most privacy friendly approach. It does not mean that pilot projects can contain the least privacy friendly approaches, as they are only considered as pilot, but on the contrary, privacy-by-design and default principles must be in place from the very beginning, whereas lessons learnt from both previous pandemic and pilot project will bolster these privacy friendly safeguards and approaches of the controllers in Spain.
- vi. Subsequently, the similar approach pertaining to publishing source code of the application and establishing a common platform where users could log their comments and complaints must definitely be leveraged to the any potential of use of these applications in the future. As discussed above, although it attracted some vulnerabilities in terms of security, we still believe that benefits derived from this approach clearly outweighs the potential risk from data protection law perspective. It gives an efficient tool to keep the application dynamic and remediate any potential gaps resulted from the technical implementation of the application, which is also in line with aforementioned idea of “playing both sides of the game”. As such, we are of view that open-source-code approach should be applied to keep the list of potential bugs and vulnerabilities, as it would support both transparency, user engagement and attracts views of technical

experts in the field, which would keep security of processing activities, in line with the GDPR principles¹⁸⁵⁷.

- vii. Pertaining to the lawful basis, we believe that creating a more room for user/data subject consent for the processing activities would be more in line with the GDPR and Ley Orgánica 3/2018 approach. As discussed across the chapters, data controllers will still be obliged to rely on other lawful basis due to the nature of the processing activities, but sustaining volunteerism for both the use of the application and type of data to be provided to the public authorities will open the doors for more consent-based approach, which should be maintained and remediated, if possible. The similar approach should be applicable to the pilot project as well. Moreover, even the pilot version must not oblige any identification of data subjects during downloading the application on android or apple stores. In other words, data controllers should agree with all technology giants that any type of users will not be obliged to log in to their accounts to download these applications, contrary to what is being asked by them to download other type of applications. Although such processing is not directly under the control of Spanish data controllers, there are still partial responsibility of them as well, due to the unique nature of the situation and processing activities. Thus, tech giants could be asked to create exceptions for the contact tracing applications, so that users ID will not be reached by any party at all, only because they download these applications. Users will have control over their personal data and will disclose only

¹⁸⁵⁷ See respectively Article 32 of the GDPR, security of processing; recital 78 of the GDPR, appropriate technical and organizational measures; recital 83 of the GDPR, security of processing.

the portion of the data they deem necessary to relevant authorities, in line with the GDPR ¹⁸⁵⁸ and Ley Orgánica 3/2018¹⁸⁵⁹ approach.

- viii. Moreover, considering the necessities that are detailed in Chapter 6 pertaining to the need for more detailed and elaborate responsibilities on controller and processors side stipulated within the agreements between public authorities published, Spanish authorities that intend to utilize these applications again must clearly determine those responsibilities and accountabilities in their processing activities. Both data processing agreements ¹⁸⁶⁰ and service agreements must stipulate these in detail. Also, the Orders as well as the regulations passed and published pertaining to the use of these applications again must point out the privacy necessities, and clearly set out the roles and accountabilities of each public institution in such extreme cases with relevant data protection references. It is definitely crucial part of processing activities from the beginning from organizational and administrative perspective, given that this documentation is sort of creating the constitution of processing activities that resulted from

¹⁸⁵⁸ Both the EDPS and the EDPB regularly issue statements and opinions on various aspects of data protection, including the rights of data subjects. These statements often emphasize the importance of individuals having control over their personal data and the obligations of organizations to respect and protect these rights in accordance with the GDPR. These are, for instance:

“EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak” available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en

“EDPS Opinion on the European Commission’s Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)” available at: https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf (accessed on 15 February 2024).

¹⁸⁵⁹ AEPD also provides guidelines and recommendations regarding data protection, which often emphasize the control of data subjects over their personal data. These are, for example;

“Guía sobre el uso de videocámaras para seguridad y otras finalidades” available at: <https://www.aepd.es/guias/guia-videovigilancia.pdf> (accessed on 15 February 2024).

AEPD (2021) “Guide on Use of Cookies” available at: <https://www.aepd.es/documento/guia-cookies-en.pdf> (accessed on 15 February 2024).

¹⁸⁶⁰ ICO also reiterated the importance of determining processor and controller responsibilities in a written agreement by stating that when a controller engages a processor to handle personal data on their behalf, it is essential for both parties to have a formal written contract. Likewise, if a processor enlists the assistance of another entity (i.e., a sub-processor) to aid in personal data processing for a controller, a written contract must also be established with the sub-processor. These contracts serve to ensure that both controllers and processors comprehend their respective obligations, responsibilities, and liabilities. For the full information see ICO Website, Contracts available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/contracts/> (accessed on 23 June 2024).

digital contact tracing. Thus, it is of massive importance to articulate these roles, responsibilities, and accountabilities at the outset of contemplated processing activities in all formal documents that are related to processing activities. We believe that the checklist provided by the EDPS¹⁸⁶¹ would perfectly assist Spanish data controllers in this regard as well. This list comprises all the necessities that are needed to be considered for the envisaged processing activities on a high level, which will definitely reduce the amount of ambiguity in terms of the necessities required in these documents. This strict and elaborate approach must also be reflected on the processing arrangements with third party service provided technology companies due to the discussed concerns of the users. It will help data controllers to exert more power on the personal data accessed by third parties, if any, so that they will remain in full control of the processing activities and individuals in society would not have worry about abuse of their personal data by third parties. These necessities can be supported by the privacy friendly methodologies we have discovered in Chapter 3 and 4 for other European applications, such as due diligence mechanism and ongoing oversight of processing activities by data controller during each step of third-party involvement.

- ix. Lastly, with regards to the implementation of data subject rights, the final approach of controllers of the Radar Covid application, namely providing forms and website links to contact and submit a request must be maintained for the any potential use of these applications. It is important to remember that even if the applications does not process any identifiable data, it is still important to provide data subjects with the option of submitting request for the implementation of the most essential rights under the GDPR and Ley Orgánica 3/2018, namely

¹⁸⁶¹ For the full checklist prepared by the EDPS, see “Checklist 3: What is required in a processing agreement?” available at: https://www.edps.europa.eu/sites/default/files/publication/19-09-27_checklist_3requirements_processing_en.pdf (accessed on 15 February 2024).

right to information¹⁸⁶², right of access¹⁸⁶³, right to rectification¹⁸⁶⁴, right to erasure (right to be forgotten)¹⁸⁶⁵ and right to object¹⁸⁶⁶. The reason is that user of relevant application (data subjects) have the right to obtain confirmation as to whether their non-identifiable data is being processed and, if so, to access that data, or to request correction, or deletion of this non-identifiable data, and to object further processing of this data, such as phone numbers or email address of users without any further identification associated, such as full name or ID number. Therefore, all documentation of applications, particularly the privacy notice, should clearly articulate these rights and its applicability to specific context with real life examples, so that users can have better understanding of potential uses cases in real life. Furthermore, assigning a DPO for both implementation of data subject requests, and inclusion for other required parts in line with the GDPR requirements¹⁸⁶⁷ would solidify the efficient implementation of data protection compliance activities of the controllers. By providing these necessities, at minimum, data controllers could at least have another chance to provide clear information about non-existence of any identifiable data being processed by relevant application, which would therefore support the privacy-friendly approach of the controllers. From more overarching perspective, similar to above, we would like to reiterate the importance of modernizing the healthcare and pandemic legislation and creating more room for data protection/right to privacy of individuals, with the accountabilities and responsibilities of governments to protect these data subject rights, and restrictions of

¹⁸⁶² For the full articles see Articles 12-14 of the GDPR and Ley Orgánica 3/2018.

¹⁸⁶³ For the full articles see Articles 15 of the GDPR and Ley Orgánica 3/2018.

¹⁸⁶⁴ For the full articles see Articles 16 of the GDPR and Ley Orgánica 3/2018.

¹⁸⁶⁵ For the full articles see Articles 17 of the GDPR and Ley Orgánica 3/2018.

¹⁸⁶⁶ For the full articles see Articles 21 of the GDPR and Ley Orgánica 3/2018.

¹⁸⁶⁷ See Article 37 of the GDPR, Designation of Data Protection Officer; Recital 97 of the GDPR, Data Protection Officer; Article 37 of Ley Orgánica 3/2018, Intervención Del Delegado de Protección de Datos En Caso de Reclamación Ante Las Autoridades de Protección de Datos.

other important rights that might be impacted from the pandemic as well.

Overall, although Spanish controller did not fully fail in terms of data protection law compliance, there seems to be some room for enhancement due to the complexity of its legal framework and quickly evolving nature of technology and pandemic itself in line with the AEPD decisions. Hence, it is plausible to conclude that the lessons learned from digital contact tracing activities in Spain during the pandemic underscore the importance of a holistic approach that combines technological innovation with regulatory engagement, and a commitment to privacy and data protection law requirements. These pinpoint lessons learnt should be supported by the technical and organizational measures and methodologies we have discovered in Chapter 3 and 4 for other European applications in the future, with the updated approach of AEPD and regulators for pandemic and data protection requirements.

Conclusions

As discussed through the entire work in line with our research question presented in the introduction part, we have undertaken a comprehensive examination of privacy/data protection law aspects of Spanish and European contact tracing applications, aiming to assess their data protection risks, and evaluate the controllers' compliance efforts, and propose innovative solutions to mitigate privacy threats on more efficient basis in the future use of these applications, considering that rapid adoption of these technologies and constantly evolving nature of pandemic has brought to the forefront a myriad of privacy concerns and regulatory challenges.

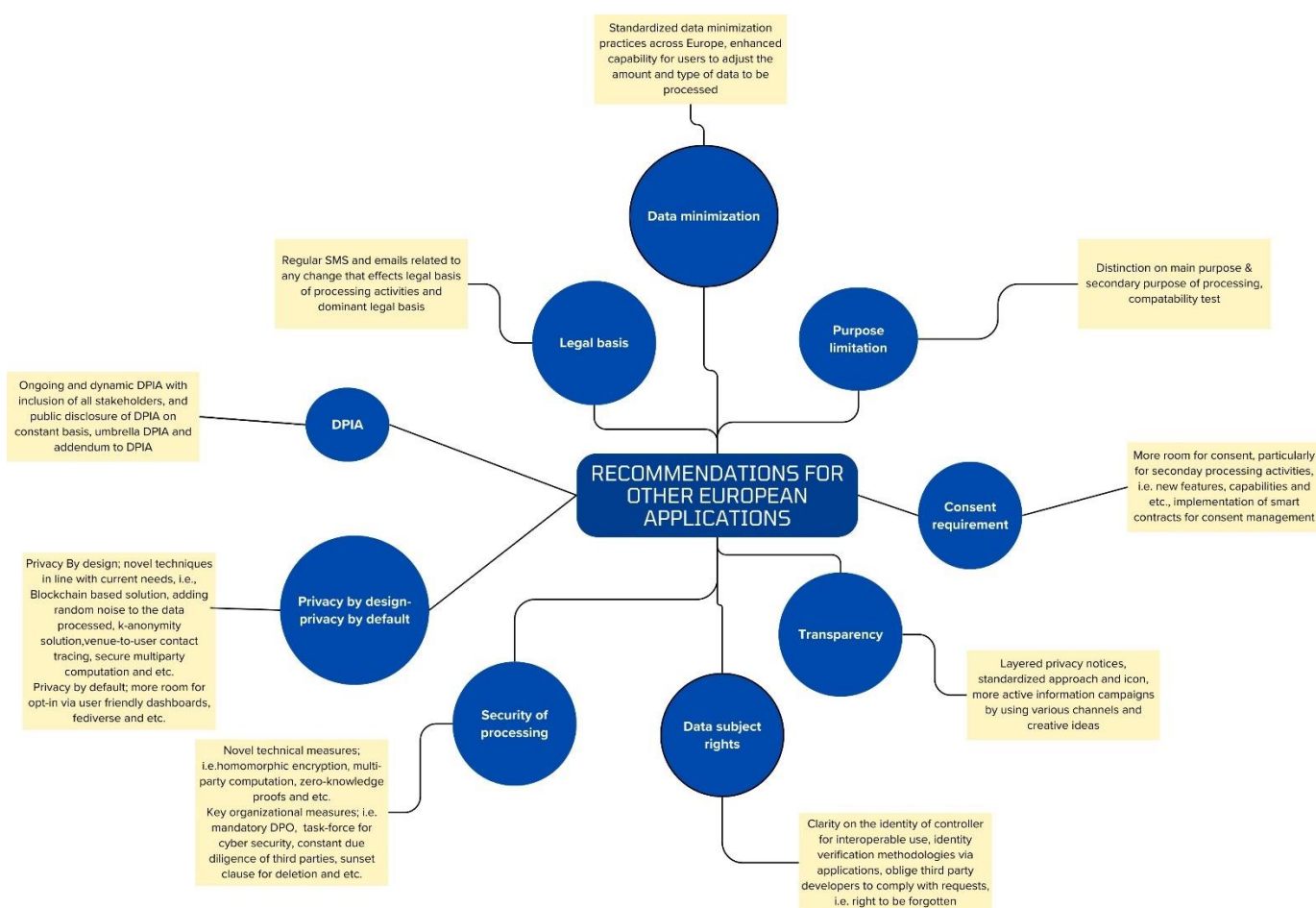
Accordingly, the journey through the intricacies of contact tracing privacy, it became evident that the extensive collection and storage of personal data by contact tracing apps pose significant risks to user privacy, as raised in the literature prior to our research. To summarize these points, the aggregation of sensitive information, including location data, health status, and social interactions raised concerns regarding unauthorized access, data breaches, and potential misuse of users' personal data. Moreover, centralized data storage and processing mechanisms created single points of failure vulnerable to hacking or governmental surveillance, further exacerbated privacy risks, as we elaborated and presented in Chapter 2. Similarly, certain vulnerabilities of decentralized model, in conjunction with advanced re-identification of data subjects could multiply the risk posed by the applications. On the top of that, problematic points on voluntariness of the applications, as well as the perceived risks of data subjects did also impact the data protection aspects of contact train applications.

Hence, amidst these challenges, we understood that compliance with data protection regulations such as the GDPR, ePrivacy Directive and LOPDyGDD represents a critical cornerstone in safeguarding user privacy to mitigate such risks. To this end, this research examined the compliance efforts of each data controller in EEA and Spain by reviewing their privacy policies, technical specifications, terms and conditions documents as well as reported cases to the supervisory authorities with regards to their activities till our date, and the EU data and reports on the applications. On the back of these analyses, each

section of our thesis delved deeper into these aspects, providing specific examples, data, case studies, and expert opinions in the remit of data protection law to support the discussions, which we believe could be leveraged to the further use of the applications in Spain and the EEA/EU in general. Correspondingly, as elaborated across the research, we concluded that it is almost impossible to comply with each and all necessities of data protection requirements at once, due to the unexpected nature of the pandemic and short development time of the applications, even though most of the controllers tried to perform a thorough compliance in line with the high level GDPR requirements. Thus, we understood that the dynamic and rapidly evolving nature of technology and unexpected nature of infectious disease poses significant challenges to achieving full regulatory compliance, particularly in the pandemic situation. As such, we noticed that the multifaceted nature of privacy risks, coupled with the multiparty stakeholder environment for the development of contact tracing applications, underscores the complexity of achieving compliance in privacy practices across different jurisdictions with the standstill and high-level privacy preserving methodologies, due to the general nature of regulations. In order to precisely response our research questions delineated in in the introduction in this regard, while it is possible to implement contact tracing activities in a privacy friendly manner, it is only possible to accomplish this goal by considering and implementing certain necessities.

To this end we are of view that while compliance activities of the controllers seemed to create a good-willed approach, it is not sufficient on its own to address the myriad of privacy challenges inherent in contact tracing applications. Thus, we presented a proactive technical and organizational measures approach that emphasizes the implementation of cutting-edge privacy solutions to mitigate risks and uphold privacy principles in the digital age on an ongoing basis to be well prepared from data protection law perspective for the future use of these applications, instead of ruling out the use of the applications due to existing data protection risks. For this reason, throughout this research, we first, in Chapter 1, introduced the general aspects of the contact tracing applications, alongside with use case scenarios across the world, and run the high-level introduction of data protection requirements applicable to the digital contact tracing activities. Following to

the general introduction on the applications' features and applicable data protection principles, in Chapter 2, we delineated the digital contact tracing specific risks alongside with the general data protection risks applicable to any type of digital application collecting user location to perceive the potential threats being generated by the applications more accurately to address those red flags by considering the existing compliance activities of the data controllers. Thus, after determining the existing risks and compliance efforts of controllers, in the following chapters, we have delineated a range of innovative privacy-enhancing technologies and methodologies that hold promise in bolstering the resilience of contact tracing systems against privacy threats, which could also allow controllers to respond with quickly changing nature of technology and pandemic requirements.



In more detail, across the Chapter 3, 4 and 5, where we provided the main contribution for the EEA/EU perspective, most of which were not elaborated

in the existing literature from, contact tracing and data protection perspective, we delineated range of organizational measures that solidify ongoing communication with local and EU cyber security and data protection authorities to update technical requirements. Likewise, discovered ongoing and transparent DPIA with implementation and publishing of umbrella DPIAs and its addendums, and ongoing audit mechanisms with straightforward implementation methods to track the risks and success of the associated safeguards, or contractual mechanisms to oblige all tech companies involved to the process to act as quick as controllers for such unforeseen issues. Within the similar vein, we also proposed detailed communication and awareness campaigns by offering promotion of transparency and accountability in data collection and usage practices as it is crucial in building trust and confidence among users, by providing clear and accessible information solutions about data handling practices, to empower users to make informed decisions about their privacy and consent preferences, such as nuances of standardized privacy notices solution, and layered notices, as well as open-source code approach to solidify such transparent approach. Furthermore, due diligence, obligatory designation of DPO, and user-friendly opt-in dashboards solutions for privacy by default approaches for controllers to be ready in advance of any potential use of the applications as much as possible by discussing the feasibility of different views in different literature of data protection or other law and technology remit, or by leveraging the existing case law and decisions of data supervisory authorities as detailed in the introduction. Also, as part of these organizational upgrades, we delivered certain solutions for the implementation of data subject rights, which are of massive importance to the user trust as well.

In addition to these organizational measures delineated, we also explored technical methods used in different areas that could be leveraged to privacy by design and technical and organizational measures within the sense of the GDPR and LOPDyGDD. Although some of these methods were used in different contexts of data protection compliance matters, we, more specifically, explored the adoption of federated learning approaches to mitigate privacy risks associated with centralized data storage and processing and enabling collaborative data analysis without compromising individual privacy rights within the contact tracing context. Similarly, discussed the

feasibility of blockchain technology for data minimization and consent management activities to reduce risks of re-identification and excessive data processing. Likewise, as part of these measures, we have also explored new approaches and methods for other known techniques in data protection literature such as homomorphic encryption for more efficient encryption practices, k-anonymity for data anonymization activities to prevent any type of re-identification of users, and smart consent management tools for classical consent management approach to offer effective means of protecting sensitive personal information while preserving the efficacy of contact tracing efforts, rather than directly focusing on the general GDPR concepts.

Subsequently, considering the importance of these nuanced solutions for different portions of the compliance activities in the GDPR jurisdiction, we presented their interconnected nature, as failure to do one step would impact the success of the rest as well. In more detail, as part of privacy-by-design and default approaches discussed, instead of simply rejecting centralized methods, or pointing out classical risk scenarios that could arise with any type of tracing application, particularly use of GPS location data, we explored Secure Multiparty Computation as well as blockchain based communication as part of privacy-by-design approaches to prevent de-anonymization and re-identification of data subjects, among other cutting edge solutions.

Moreover, we also analyzed the nature of the existing guidelines on contact tracing to assess the sufficiency of compliance activities of the controllers, and success of data protection authorities/regulators as well to observe if the guidelines issued are detailed and specific enough to complement the general nature of GDPR for the pandemic context. As such, we also provided our analyses and contribution for the content and quality of the existing guidelines published by the EU agencies for the EEA applications, proposed certain improvement areas for the EU authorities and regulators issuing these guidelines, whereas analyzed the adherence of controllers to the existing guidelines as well.

Afterwards, across the last two chapters of our research, we investigated the detailed aspects of digital contact tracing activities by starting from the efficiency of pandemic laws in Spain and discussed potential need for enacting new laws and regulations on pandemic management, and its

interplay with data protection aspects of the pandemic. More specifically, we applied more holistic approach on the entire pandemic and data protection situation and data protection aspects contact tracing application as a new approach, since such holistic approach could be more supportive to address data protection matters resulted from the applications on both regulators and controllers' level. To this end, constitutional court decision on the legality of pandemic limitations, details of the Orders dealing with pandemic and digital applications used therein, as well as the implementation of data protection requirements during that period were analyzed, considering the regulatory requirements. Accordingly, as the main contribution of Chapter 6, we provided main takeaways for regulators to revamp the regulations in line with our current era's needs, particularly on data protection aspects to facilitate future implementation of data protection matters during pandemics. Moreover, the comprehensive lawful basis selection of Spain for the contact tracing application was evaluated as well, considering the wide range of lawful basis could have an impact on the flexibility of processing activities as detailed in relevant chapters. As such, following these assessments on the legal aspects of the pandemic and data protection matters, tailor made solutions provided to both regulators and data controllers for the future management of data protection issues in Spain in the future.

In the last chapter of our research, security vulnerabilities as well as data protection implementation of Radar Covid were analyzed in light of the technical specifications and relevant documentation of the application, as well as AEPD's guidelines, and tailor-made solutions were provided accordingly for each specifics identified regarding these vulnerabilities and implementational matters. Additionally, to pinpoint the lessons learned for both data controllers and regulators in Spain as part of their future digital contact tracing activities, the AEPD's decisions on Radar Covid application was analyzed in detail and provide conclusions. Finally, as detailed above, comprehensive list of lessons learned for future contact tracing applications to be used in Spain was provided for the ease of reference for future data controllers and/or regulators to pinpoint our main contribution to the data protection literature in Spain legal landscape.

Thus, on the back of these analysis implemented for both the EEA and Spanish applications, instead of simply highlighting the criticalness of inherent risks and pointing finger to the controllers for the parts they fell short of the data protection requirements, we explored the importance of cutting edge privacy enhancing safeguards, i.e. technical and organizational measures under the GDPR, and need for detailed ongoing guidance of the data protection supervisory authorities/regulators on both EEA/EU and local level, which will play a vital role in, fostering a culture of privacy by design and default in the development and deployment of contact tracing technologies. Therefore, as part of our research question, it is plausible to state that we explored key takeaways for data protection supervisory authorities/regulators as well, particularly in oversight and guidance mechanism as detailed in Chapter 5, and relevant parts of Chapter 6 and 7.

Overall, considering our findings and proposals, it is plausible to conclude that this research is supportive of the idea that it is possible to have privacy-friendly contact tracing applications in the future by mitigating the risks and compliance failures delineated. Accordingly, in order to achieve this target, this research underscores the imperative of proactively addressing privacy risks inherent in contact tracing applications by applying most novel privacy friendly technical and organizational measures in line with the nature of pandemic, particularly within the Spanish and European contexts, instead of simply banning the use of the applications, as there are always data protection risk at stake when it comes to use of tracing applications. Suitably, to achieve privacy friendly use of the applications, our main finding is that while data controllers' compliance activities created a foundational element as is, there is a room for the improvement in mitigating the multifaceted privacy challenges posed by these technologies due to the aforementioned reasons. Through an exploration of innovative privacy-enhancing measures and the promotion of transparency, accountability, and stakeholder collaboration, and all the other solutions we explored for digital contact tracing applications under the European and Spanish regime, we advocated for a comprehensive approach to safeguarding individual privacy rights amidst the imperatives of public health surveillance by establishing novel and up-to-date technical and organizational safeguards on an ongoing basis, under the detailed and up-to-date guidance of data protection authorities. By bridging regulatory

requirements with cutting-edge solutions, we believe it is possible to provide actionable insights to navigate the intricate intersection of data protection laws and contact tracing applications within Spain and Europe.

Hence, as the main targeted contribution of our work to the existing data protection law literature, as we look towards the future, we defend the idea that it is essential to recognize that safeguarding data protection in contact tracing applications on an ongoing and collaborative endeavor instead of either simply out ruling the use of the apps due to the risks presented thereby, or limiting the compliance activities with the generic data protection safeguards to achieve the most privacy friendly version thereof. To this end, we would also like to underline the idea that such endeavor requires a concerted effort from data controllers and policymakers. By embracing a holistic approach that integrates technological innovation with regulatory guidance and oversight, it is possible to foster a culture of data protection and trust in contact tracing technologies, ensuring that they serve as effective tools in protecting public health while respecting individual privacy rights. Therefore, while there are risks associated with use of contact tracing applications, and some potential gaps in data controllers' compliance activities with the European and Spanish privacy legal landscape, we are of view that considering the importance of implementing such technological tools, the most accurate response to the threats would be to respond more cutting edge privacy solutions in the form of technical and organizational measures as explored on this research to those threats to ensure there are no risks posed to data subjects, and thereby, enhancing data controllers' compliance with the respective rules in the GDPR and Spanish jurisdiction in the future. Therefore, this thesis targeted to provide a guidance for the future data controllers, and regulators for their implementation of privacy friendly applications, if needed, and humbly aimed to provide a contribution to the existing literature by creating more privacy friendly contact tracing atmosphere instead of only highlighting the risks posed.

REFERENCES

Articles and Books:

- Acar, Abbas; Aksu, Hidayet; Uluagac, A. Selcuk; and Conti, Mauro (2018) "A survey on homomorphic encryption schemes: Theory and implementation", *ACM Computing Surveys (Csur)* 51, no. 4, pp.1-35.
- Agrawal, Divyakant; Bernstein, Philip; Bertino, Elisa; Davidson, Susan, Dayal, Umeshwas; Franklin, Michael; Gehrke, Johannes; Haas, Laura; Halevy, Alon; Han, Jiawei; Jagadish, H.V.; Labrinidis, Alexandros; Madden, Sam; Papakonstantinou, Yannis; Patel, Jignesh; Ramakrishnan, Raghu; Ross, Kenneth; Shahabi, Cyrus; Suciu, Vaithyanathan, Shiv; and Widom, Jennifer (2011) *Challenges and opportunities with Big Data*, Purdue University (Purdue e-Pubs), Cyber Center Technical Reports, 2011-1, p.1-16.
- Ahmed, Nadeem; Michelin, Regio A.; Xue, Wanli; Ruj, Sushmit; Malaney, Robert; Salil S. Kanhere, Seneviratne, Aruna; Hu, Wen; Janicke, Helge and Sanjay K. Jha (2020) "A survey of COVID-19 contact tracing apps", *IEEE access* 8, pp.134577-134601.
- Alrawais, Arwa; Alharbi, Fatemah; Almoteri, Moteeb; Altamimi, Beshayr; Alnafisah, Hessa and Aljumeiah, Nourah (2022) "Privacy-Preserving Techniques in Social Distancing Applications: A Comprehensive Survey", *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol.26, n. 3, pp. 325-34.
- Alshawi, Amany; Al-Razgan, Muna; AlKallas, Fatima H; Bin Suhaim, Raghad Abdullah; Al-Tamimi, Reem; Alharbi, Norah and AlSaif, Sarah Omar (2022) "Data privacy during pandemics: a systematic literature review of COVID-19 smartphone applications", *PeerJ Computer Science*, vol.7, e826, pp.1-29. doi: 10.7717/peerj-cs.826. PMID: 35111915; PMCID: PMC8771796.
- Álvarez García, Vicente J. (2020) "El coronavirus (COVID-19): respuestas jurídicas frente a una situación de emergencia sanitaria", *El Cronista del Estado Social y Democrático de Derecho*, monográfico Coronavirus... y otros problemas, marzo-abril 2020, pp. 6-21, pp. 12-13.
- Álvarez Vélez, M. Isabel (2021) "Alarm and pandemic: legal-constitutional problems of states of necessity in light of the doctrine of the Constitutional Court: Comments on the Constitutional Court Ruling 148/2021, of July 14, unconstitutionality appeal no. 2054-2020. (BOE no. 182, of July 31, 2021); to the Ruling of the Constitutional Court 183/2021, of October 27, unconstitutionality appeal no. 5342-2020. (BOE no. 282, of November 25, 2021); and to the Ruling of the Constitutional Court 168/2021, of October 9. Appeal for protection no. 2109-2020. (BOE no. 268, of November 9, 2021)", *Magazine of the Cortes Generales*, n. 111, pp. 547-574.
- Ami, Junko; Ishii, Kunihiro; Sekimoto, Yoshihide; Masui, Hiroshi; Ohmukai, Ikki; Yamamoto, Yasunori and Okumura, Takashi (2021) "Computation of infection risk via confidential locational entries: A precedent approach for contact tracing with privacy protection", *IEEE Access* 9, pp.87420-87433.
- Amoedo-Souto, Carlos Alberto (2020) "Vigilar y castigar el confinamiento forzoso: problemas de la potestad sancionadora al servicio del estado de alarma sanitaria", *El Cronista del Estado Social y Democrático de Derecho*, n. 86-87, pp. 66-77.
- Andreu Martínez, Belén (mayo 2020) "Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19", *Actualidad Jurídica Iberoamericana*, n. 12 bis, pp. 848-859.
- Andreu-Perez, Javier; Poon, Carmen CY; Merrifield, Robert D.; Wong, Stephen TC and Yang, Guang-Zhong (2015) "Big data for health.", *IEEE journal of biomedical and health informatics*, vol.19, n. 4, pp.1193-1208.

- Ang, Vincent, and Lwin Khin, Shar (2021) "Covid-19 one year on—security and privacy review of contact tracing mobile apps", *IEEE Pervasive Computing*, vol. 20, no. 4, pp.61-70.
- Anglemeyer Andrew; Moore, Theresa HM; Parker, Lisa; Chambers, Timothy; Grady, Alice; Kellia Chiu et al (2020) "Digital contact tracing technologies in epidemics: a rapid review", *Cochrane Database of Systematic Reviews*, Vol. 8, Issue 8, pp.1-44, doi: 10.1002/14651858.CD013699. PMID: 33502000; PMCID: PMC8241885.
- Antignac, Thibaud and Le Métayer, Daniel (2014) "Privacy by design: From technologies to architectures", *Annual privacy forum*, Springer, Cham, pp. 1-17..
- Arenas Ramiro, Mónica (2021) "Nuevas tecnologías y retos para la protección de datos personales en Europa: el rastreo de contactos durante la pandemia por covid-19", *Confluências| Revista Interdisciplinar de Sociologia e Direito*, vol. 23, n. 2, pp. 99-17.
- Aslam, Bakhtawar; Javed, Abdul Rehman; Chakraborty, Chinmay; Nebhen, Jamel; Raqib, Saira and Rizwan, Muhammad (2021) "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic", *Personal and ubiquitous computing*, n.22, pp. 1-17.
- Aszodi, Nikolett; Galaski, Jascha; Konoplia, Oleksandra and Reich, Orsolya (2021) "COVID-19 Technology in the EU: A Bittersweet Victory for Human Rights", *Civil Liberties Union for Europe*, Berlin, pp.1-77.
- Ausloos, Jef; Kindt, Els; Lievens, Eva; Valcke, Peggy and Dumortier, Jos (2013), "Guidelines for privacy-friendly default settings", *ICRI Research Paper*, n. 12, pp.1-34, Available at SSRN: <https://ssrn.com/abstract=2220454> or <http://dx.doi.org/10.2139/ssrn.2220454>
- Azad, Muhammad Ajmal; Arshad, Junaid; Akmal, Syed Muhammad Ali; Riaz, Farhan; Abdullah, Sidrah; Imran, Muhammad and Ahmad, Farhan (2020) "A first look at privacy analysis of COVID-19 contact-tracing mobile applications", *IEEE Internet of Things Journal* 8, no. 21, pp.15796-15806.
- Bardus, Marco; Al Daccache, Melodie; Maalouf, Noel; Al Sarih, Rayan and Imad H. Elhaji (12-07-2022) "Data Management and Privacy Policy of COVID-19 Contact-Tracing Apps: Systematic Review and Content Analysis", *JMIR Mhealth Uhealth*, vol. 10, n.7, e35195, pp.1-20, DOI: 10.2196/35195, PMID: 35709334; PMCID: PMC9278406.
- Baruh, Lemi; Secinti, Ekin and Cemalcilar, Zeynep (2017) "Online privacy concerns and privacy management: A meta-analytical review", *Journal of Communication*, vol.67, no. 1, pp. 26-53.
- Bay, Jason; Kek, Joel; Tan, Alvin; Hau, Chai Sheng; Yongquan, Lai; Tan, Janice and Anh Quy, Tang (2020) "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders", *Government Technology Agency-Singapore, Tech. Rep*, Vol. 18, no. 1, pp. 1-9.
- Becker, Regina; Thorogood, Adrian; Ordish, Johan and Beauvais, Michael JS. (2020) "COVID-19 research: navigating the European general data protection regulation", *Journal of Medical Internet Research*, vol. 22, no. 8, e19799, pp.1-9.
- Bengio, Yoshua; Ippolito, Daphne; Janda, Richard; Jarvie, Max; Prud'homme, Benjamin; Rousseau, Jean-François; Sharma, Abhinav and Yu, Yun William (2021) "Inherent privacy limitations of decentralized contact tracing apps", *Journal of the American Medical Informatics Association*, vol. 28, no. 1, pp. 193-195.
- Bengio, Yoshua; Janda, Richard; Yu, Yun William; Ippolito, Daphne; Jarvie, Max; Pilat, Dan; Struck, Brooke; Krastev, Sekoul and Sharma, Abhinav (2020) "The need for privacy with public digital contact tracing during the COVID-19 pandemic", *Lancet Digit Health*, vol. 2, n.7, doi: 10.1016/S2589-7500(20)30133-3. Epub 2020 Jun 2. PMID: 32835192; PMCID: PMC7266569., pp. e342-e344.

- Berman, Gabrielle; Carter, Karen; Garcia Herranz, Manuel and Sekara, Vedran (2020) *Digital contact tracing and surveillance during COVID-19, General and child-specific ethical issues*, UNICEF Office of Research, Office of Research-Innocenti Working Paper, pp. 1-26.
- Besik, Saliha Irem and Freytag, Johann-Christoph (2020) "Managing Consent in Workflows under GDPR", *ZEUS Workshop 2020*, in Manner, Johannes; Haarmann, Stephan; Kolb, Stefan; and Kopp, Oliver (eds.), CEUR Workshop Proceedings, n. 2575, pp. 18-25.
- Bieker, Felix; Friedewald, Michael; Hansen, Marit; Obersteller, Hannah and Rost, Martin (2016) "A process for data protection impact assessment under the European general data protection regulation", *Annual Privacy Forum*, Springer, Cham, pp. 21-37.
- Blasi Casagran, Cristina, and Cañabate Pérez, Josep (2024) *Legislación y derecho digital para no juristas*. Servei de Publicacions de la Universitat Autònoma de Barcelona. (preview version available at Google Scholar),
- Blasimme, Alessandro; Ferretti, Agata and Vayena, Effy (2021) "Digital contact tracing against COVID-19 in Europe: current features and ongoing developments", *Frontiers in Digital Health*, vol. 3, 660823, pp.1-10, doi: 10.3389/fdgth.2021
- Bobbio, Andrea; Campanile, Lelio; Gribaudo, Marco; Iacono, Mauro; Marulli, Fiammetta and Mastroianni, Michele (2023) "A cyber warfare perspective on risks related to health IoT devices and contact tracing", *Neural Computing and Applications*, vol. 35, n. 19, pp. 13823-13837, doi: <https://doi.org/10.1007/s00521-021-06720-1>,
- Bosch, Xavier (2002) "Spain decentralises its healthcare system (news roundup)", *British Medical Journal*, vol. 324, n. 7329, pp.68-69.
- Boutet, Antoine; Castelluccia, Claude; Cunche, Mathieu; Lauradou, Cédric; Roca, Vincent; Baud, Adrien and Raverdy, Pierre-Guillaume (2022) "DESIRE: Leveraging the best of centralized and decentralized contact tracing systems", *Digital Threats: Research and Practice (DTRAP)*, vol. 3, n. 3, pp.1-20.
- Bradford, Laura; Aboy, Mateo and Liddell, Kathleen (2020) "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes", *Journal of Law and the Biosciences*, vol. 7, n. 1, Isaa034, pp.1-21.
- Breen, Stephen; Ouazzane, Karim and Patel, Preeti (2020) "GDPR: Is your consent valid?" *Business Information Review*, vol. 37, no. 1, pp.19-24.
- Bygrave, Lee (2017) "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements", *Oslo Law Review*, vol.1, pp.105-120. 10.18261/issn.2387-3299-2017-02-03.
- Calzolaio, Simone (2016) "Digital (and privacy) by default. Constitutional identity of e-government/Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale", *Journal of Constitutional History (Giornale di Storia Costituzionale)*, vol. 31, pp.185-206.
- Campillo Pérez, Lorena (2023) "La tecnología de localización aplicada a la investigación científica: el cumplimiento normativo en torno a la protección de datos personales" *Revista de Derecho Político*, vol. 117, pp. 311-340.
- Carnovale, Maria, and Louisy, Khahlil (2021) "Public Health, Technology, and Human Rights: Lessons from Digital Contact Tracing", *arXiv preprint arXiv:2107.07552*, pp. 1-23.
- Cavoukian, Ann, and Jonas, Jeff (2012) "Privacy by Design in the Age of Big Data", *Eurocontrol Int*, pp.1-17.
- Chakraborty, Pranab; Maitra, Subhamoy; Nandi, Mridul and Talnikar, Suprita (2020) "Contact Tracing in Post-Covid World: A Cryptologic Approach" *Indian Statistical Institute Series*, Singapore, Springer Chakraborty, vol.10, 1007/978-981-15-9727-5, pp.1-134.

- Chan, Eugene Y., and Saqib, Najam U. (2021) "Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high", *Computers in Human Behavior*, vol. 119, 106718, pp.1-13.
- Chan, Justin; Foster, Dean; Gollakota, Shyam; Horvitz, Eric; Jaeger, Joseph; Kakade, Sham; Kohno, Tadayoshi et al. (2020) "Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing", *arXiv preprint arXiv:2004.03544v4*, PPR:PPR268538, pp.1-22.
- Cho, Hyunghoon; Ippolito, Daphne and Yu, Yun William (2020) "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." *arXiv preprint arXiv:2003.11511*, pp.1-12.
- Chopdar, Prasanta Kr. (2022) "Adoption of Covid-19 contact tracing app by extending UTAUT theory: Perceived disease threat as moderator", *Health Policy and Technology*, vol. 11, no. 3,100651, pp. 1-13.
- Chowdhury, Mohammad Javed Morshed; Ferdous, Md Sadek; Biswas, Kamanashis; Chowdhury, Niaz and Muthukkumarasamy, Vallipuram (2020) "COVID-19 contact tracing: challenges and future directions", *IEEE Access*, vol. 8, pp. 225703-225729.
- Clarke, Roger (2009) "Privacy impact assessment: Its origins and development", *Computer law & security review*, vol. 25, no. 2, pp. 123-135.
- Clarkson, Gavin; Jacobsen, Trond E. and Batcheller, Archer L. (2007) "Information asymmetry and information sharing", *Government Information Quarterly*, vol. 24, no. 4, pp.827-839.
- Cotino Hueso, Lorenzo (2021) "La (in)constitucionalidad de las restricciones y suspensión de la libertad de circulación por el confinamiento frente a la covid", en Garrido López, C. (coord.) *Excepcionalidad y Derecho: el estado de alarma en España*, Colección Obras colectivas, Fundación Manuel Giménez Abad, Zaragoza, pp. 159-195.
- Cranor, Lorrie Faith (2012) "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice", *J. on Telecomm. & High Tech. L.*, vol. 10, pp. 273-308.
- Dash, Sidhartha Sekhar and Modi, Ronak, (2019) "Role of Psychology in Legal Studies", *JETIR*, Volume 6, Issue 5, pp.2557-2562.
- De Gatta Sánchez Fernández, Dionisio(2020) "Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el covid-19 y sus prórrogas", *AIS: Ars Iuris Salmanticensis*, vol. 8, no. 2, pp. 192-199.
- De la Cruz Mena, Víctor (2020) *Implicacions ètiques del big data en la sanitat pública*, Universidad Autonoma de Barcelona, Diposit Digital de documents de la UAB de la <https://ddd.uab.cat/record/231494> (accessed on 8 June 2024).
- De Montjoye, Yves-Alexandre, Tarun Ramadorai, Tommaso Valletti, and Ansgar Walther (2021) "Privacy, adoption, and truthful reporting: a simple theory of contact tracing applications", *Economics Letters*, vol. 198, pp. 109676.
- Di Marco, Piergiuseppe; Park, Pangun; Pratesi, Marco and Santucci, Fortunato (2021) "A Bluetooth-Based Architecture for Contact Tracing in Healthcare Facilities", *Journal of Sensor and Actuator Networks*, vol. 10, n. 2, pp.1-15.
- Domínguez Álvarez, José Luis (2020) "La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19", *Revista de Comunicación y Salud*, vol.10, n. 2, pp. 607-624.
- Domínguez Álvarez, José Luis (2020) "Desafíos de las Administraciones Públicas para garantizar el derecho fundamental a la protección de datos personales en la era post-COVID-19.", *Revista Eurolatinoamericana de Derecho Administrativo*, vol. 7, núm. 1, pp. 167-191.

- Domínguez Álvarez, José Luis (2020) "Public Administration's Challenges in Order to Guarantee the Fundamental Right of Personal Data Protection in the Post-COVID-19 Era", *Revista Eurolatinoamericana de Derecho Administrativo*, vol. 7, núm. 1, pp. 167-191.
- Domínguez Álvarez, José Luis (2020) "Privacidad y salud pública. Una simbiosis compleja pero necesaria para hacer frente a la Covid-19", *AIS: Ars Iuris Salmanticensis*, vol. 8 n.2, pp. 200–206.
- Du, Li; Raposo, Vera Lúcia and Wang, Meng (2020) "COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the Gap for International Pandemic Control", *JMIR Mhealth Uhealth*, vol.8, n.11, pp.1-10. doi: [10.2196/23194](https://doi.org/10.2196/23194) PMID: [33156804](https://pubmed.ncbi.nlm.nih.gov/33156804/) PMCID: [7704120](https://pubmed.ncbi.nlm.nih.gov/7704120/).
- Dubin, Kenneth A. (2021) "Spain's response to Covid-19", *Coronavirus Politics*, pp.339-260.
- Durán Alba, Juan Fernando (2021) "Afectaciones a la libertad de circulación derivadas del estado de alarma declarado a causa de la crisis «Covid-19»", en Biglino Campos, Paloma y Dyrán Alba, Juan Fernando (dirs.) *Los efectos horizontales de la Covid-19 sobre el sistema constitucional: estudios sobre la primera oleada*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, pp. 193-220.
- El Emam, Khaled, and Dankar, Fida Kamal (2008) "Protecting privacy using k-anonymity", *Journal of the American Medical Informatics Association*, vol. 15, n. 5, pp. 627-637.
- Elkhodr M, Mubin O, Iftikhar Z, Masood M, Alsinglawi B, Shahid S, Alnajjar F (2021) "Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis", *J Med Internet Res*, vol 23, n.2, pp.1-17.
- Esayas, Samson (2015) "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", *European Journal of Law and Technology*, vol. 6, n. 2, pp.1-23.
- Escobar Roca, Guillermo (2021) "Los derechos humanos en estados excepcionales y el concepto de suspensión de derechos fundamentales", *Revista de Derecho Político*, vol. 110, pp. 113-152.
- Evans, David; Kolesnikov, Vladimir and Rosulek, Mike (2018) "A pragmatic introduction to secure multi-party computation", *Foundations and Trends in Privacy and Security*, vol. 2, n. 2-3, pp. 70-246.
- Fahey, Robert A., and Hino, Airo (2020) "COVID-19, digital privacy, and the social limits on data-focused public health responses", *International Journal of Information Management*, vol.55, p.102181.
- Fernandez-Bermejo Utrilla, Dolores (2021) "Soft Law Governance in Times of Coronavirus in Spain", *Eur J Risk Regul*, vol. 12, n.1, pp.111-126.
- Ferretti, Federico (2014) "Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?", *Common market law review*, vol. 51, n. 3, pp.843-868.
- Ferretti, Luca; Wymant, Chris; Kendall, Michelle; Zhao, Lele; Nurtay, Anel; Abeler-Dörner, Lucie; Parker, Michael; Bonsall, David and Fraser, Christophe (2022) "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing", *Science* 368, n. 6491, pp.1-7.
- Fox, Grace; Clohessy, Trevor; van der Werff, Lis; Rosati, Pierangelo and Lynn, Theo (2021) "Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications", *Computers in Human Behavior*, vol. 121, pp. 1-15.
- Garousi, Vahid and Cutting, David (2021) "What do users think of the UK's three COVID-19 contact-tracing apps? A comparative analysis", *BMJ Health & Care Informatics*, vol. 28, n. 1, pp. 1-7.

- Gasser, Urs; Ienca, Marcello; Scheibner, James; Sleigh, Joanna and Vayena, Effy (2020) "Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid", *The Lancet Digital Health*, vol. 2, n. 8, pp e425-e434.
- Georgiou, Dimitra, and Lambrinouidakis, Costas (2021) "Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations", *Future Internet*, vol. 13, n. 3, pp. 1-12.
- Ghani, Norjihan Abdul; Hamid, Suraya and Udzir, Nur Izura (2016). "Big data and data protection: Issues with purpose limitation principle", *International Journal of Advances in SoComputing & Its Applications*, vol. 8, n.3, pp.116-121.
- Gosselin, Rémi; Vieu, Loïc; Loukil, Faiza and Benoit, Alexandre (2022) "Privacy and Security in Federated Learning: A Survey", *Applied Sciences*, vol. 12, n. 19, pp. 1-15.
- Guisado-Clavero, Marina; Ares-Blanco, Sara and Ben Abdellah, Lubna Dani (2021) "Using mobile applications and websites for the diagnosis of COVID-19 in Spain", *Enfermedades infecciosas y microbiología clínica (English ed.)* vol. 39, n. 9, pp.454-457.
- Gürses, Seda; Troncoso, Carmela and Díaz, Claudia (2011) "Engineering privacy by design." *Computers, Privacy & Data Protection*, vol. 14, n. 3, pp. 1-25.
- Gutiérrez Caballero, Patricia (2021) Uso por la población española de las TIC. Especial importancia durante la pandemia del Covid-19, Trabajo de fin de Grado, Universidad de Valladolid, Facultad de Comercio, <https://uvadoc.uva.es/handle/10324/51906>.
- Hassandoust, Farkhondeh; Akhlaghpour, Saeed and Johnston, Allen C. (2021) "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective", *Journal of the American Medical Informatics Association*, vol. 28, n. 3, pp. 463-471.
- Hatamian, Majid; Wairimu, Samuel; Momen, Nurul and Fritsch, Lothar (2021) "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps", *Empirical software engineering*, vol.26, pp. 1-51, <https://doi.org/10.1007/s10664-020-09934-4>
- Henriksen-Bulmer, Jane; Faily, Shamal and Jeary, Sheridan (2020) "DPIA in context: applying dpia to assess privacy risks of cyber physical systems", *Future internet*, vol. 12, n. 93, pp.1-24.
- Hernández-Orallo, Enrique; Cano, Juan Carlos; Calafate, Carlos T. and Manzoni, Pietro (2020) "Evaluating the effectiveness of COVID-19 Bluetooth-Based smartphone contact tracing applications", *Applied Sciences*, vol.10, n. 7113.
- Hernández-Quevedo, Cristina; Scarpetti, Giada; Webb, Erin; Shuftan, Nathan; Williams, Gemma A.; Okkels Birk, Hans; Jervelund, Signe Smith; Krasnik, Allan and Vrangbæk, Karsten (2020) "Effective Contact Tracing And The Role Of Apps", *TEN*, vol. 26, n. 2, pp.40-44.
- Hintze, Mike (2018) "Privacy Statements under the GDPR", *Seattle UL Rev.*, vol. 42, pp 1129-1154.
- Hobson, Stacy; Hind Michael; Mojsilovic, Aleksandra, and Varshney, Kush. R (2020) "Trust and transparency in contact tracing applications", arXiv preprint arXiv:2006.11356, <https://arxiv.org/pdf/2006.11356.pdf>, pp.1-29.
- Hoepman, Jaap-Henk (2021) "Hansel and gretel and the virus: Privacy conscious contact tracing", *arXiv preprint arXiv:2101.03241*, <https://arxiv.org/pdf/2101.03241> pp.1-29.
- Hogan, Katie; Macedo, Briana; Macha, Venkata; Barman, Arko and Jiang, Xiaoqian (2021) "Contact tracing apps: lessons learned on privacy, autonomy, and the need for detailed and thoughtful implementation", *JMIR Medical Informatics*, vol. 9, no. 7, e27449, pp.1-20.
- Hsu, Jeremy (2020) "The Dilemma of contact-tracing apps: Can this crucial technology be both effective and private?", *IEEE Spectrum*, vol.57, n. 10, p.56-59.

- Huang, Jianwei; Yegneswaran, Vinod; Porras, Phillip and Gu, Guofei (2020) "On the privacy and integrity risks of contact-tracing applications", *arXiv preprint arXiv:2012.03283*, <https://arxiv.org/pdf/2012.03283> pp.1-17.
- Huckvale, Kit; Prieto, José Tomás; Tilney, Myra; Benghozi, Pierre-Jean and Car, Josip (2015) "Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment", *BMC medicine*, vol. 13, n. 1, pp. 1-13.
- Jahmunah, Vicnesh; Sudarshan, Vidya K.; Oh, Shu Lih; Gururajan, Raj; Gururajan, Rashmi; Zhou, Xujuan; Tao, Xiaohui et al. (2021) "Future IoT tools for COVID-19 contact tracing and prediction: a review of the state-of-the-science", *International journal of imaging systems and technology*, vol. 31, n. 2, pp.455-471.
- Jalabneh, Rawan; Syed, Haniya Zehra; Pillai, Sunitha; Apu, Ehsanul Hoque; Hussein, Molla Rashied, Russell Kabir, Arafat SM Yasir; Majumder, Md Anwarul Azim; and Saxena, Shailendra K. (2021) "Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: A literature review", *Applications of Artificial Intelligence in COVID-19*, pp. 389-404.
- Jasmontaite, Lina; Kamara, Irene; Zanfiri-Fortuna, Gabriela and Leucci, Stefano (2018) "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", *Eur. Data Prot. L. Rev.*, vol. 4, pp. 168- 189,
- Jiang, Ting, Yang Zhang, Minhao Zhang, Ting Yu, Yizheng Chen, Chenhao Lu, Ji Zhang, Zhao Li, Jun Gao, and Shuigeng Zhou (2022) "A survey on contact tracing: the latest advancements and challenges", *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, vol. 8, n. 2, pp.1-35.
- Joseph K. Liu; Man Ho Au; Tsz Hon Yuen , Cong Zuo , Jiawei Wang , Amin Sakzad , Xiapu Luo , Li Li, Kim-Kwang Raymond Choo (2021) "Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach", pp. 1-26.
- Kalgotra, Pankush; Gupta, Ashish and Sharda, Ramesh (2021) "Pandemic information support lifecycle: evidence from the evolution of mobile apps during COVID-19", *Journal of Business Research*, vol.134, pp. 540-559.
- Kaya, Emre Kursat (05-2020) *Safety and Privacy in the Time of COVID-19: Contact Tracing Applications*, Centre For Economics and Foreign Policy Studies, Cyber Governance and Digital Democracy, pp.1-11.
- Kędzior, Magdalena (2021) "The right to data protection and the COVID-19 pandemic: the European approach", *ERA forum*, vol. 21, n. 4, Springer, pp. 533-543.
- Khan, Shahidullslam and Hoque, AbuSayedMd (2016) "Digital health data: a comprehensive review of privacy and security risks and some recommendations", *Computer Science Journal of Moldova*, vol. 71, n. 2, pp.273-292.
- Kim, Hwang (2021) "COVID-19 apps as a digital intervention policy: a longitudinal panel data analysis in South Korea." *Health Policy*, vol.125, no. 11, pp.1430-1440.
- Kim, Youngrim; Chen, Yuchen and Liang, Fan (2023) "Engineering care in pandemic technogovernance: The politics of care in China and South Korea's COVID-19 tracking apps", *New media & society*, vol. 25, n.6, pp. 1432-1450.
- Klaine, Paulo Valente; Zhang, Lei; Zhou, Bingpeng; Su, Yao; Xu, Hao and Imran, Muhammad (2020) "Privacy preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic", *IEEE Internet of Things Magazine*, vol.3, n.3, pp. 58-63.
- Kleinman, Robert A., and Merkel, Colin (2020) "Digital contact tracing for COVID-19", *Cmaj*, vol.192, n. 24, pp. E653-E656.
- Kolasa, Katarzyna; Mazzi, Francesca; Leszczuk-Czubkowska, Ewa; Zrubka, Zsombor and Péntek, Márta (2021) "State of the art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review", *JMIR mHealth and uHealth*, vol.9, n.6, e23250, pp.1-11.

- Konečni, Vladimir J., and Ebbesen, Ebbe B. (1979) "External validity of research in legal psychology", *Law and Human Behavior*, vol.3, n. 1-2, pp.39-70.
- Kouliaridis, Vasileios; Kambourakis, Georgios; Chatzoglou, Efstratios; Geneiatakis, Dimitrios and Wang, Hua (2021) "Dissecting contact tracing apps in the Android platform", *Plos one*, vol. 16, n. 5, e0251867, pp.1-28.
- Kozyreva, Anastasia; Lorenz-Spreen, Philipp; Lewandowsky, Stephan; Garrett, Paul M.; Herzog, Stefan M.; Pachur, Thorsten and Hertwig, Ralph (2021) "Public perceptions of COVID-19 digital contact tracing technologies during the pandemic in Germany", *OSF*, pp.1-61.
- Krasnow Waterman, Karen, and Bruening, Paula J. (2014) "Big Data analytics: risks and responsibilities", *International Data Privacy Law*, vol. 4, n. 2, pp.89-95.
- Krehling, Leah, and Essex, Aleksander (2021) "A security and privacy scoring system for contact tracing apps", *Journal of Cybersecurity and Privacy*, vol.1, n.4, pp. 597-614.
- Legendre, Franck; Humbert, Mathias; Mermoud, Alain and Lenders, Vincent (2020) "Contact tracing: An overview of technologies and cyber risks", *arXiv preprint arXiv:2007.02806* <https://arxiv.org/pdf/2007.02806>, pp. 1-26.
- Leith, Douglas J., and Farrell, Stephen (2021) "Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps", *IEEE INFOCOM 2021-IEEE, Conference on Computer Communications*, pp. 1-10.
- Lenca, Marcello and Vayena, Effy (2020) "On the responsible use of digital data to tackle the COVID-19 pandemic", *Nature medicine*, vol. 26, n. 4 pp. 463-464.
- Leonardo, Maccari and Cagno, Valeria (2021) "Do we need a contact tracing app?", *Computer Communications*, vol. 166, pp. 9-18.
- Li, Jinfeng, and Guo, Xinyi (2020) "Global deployment mappings and challenges of contact-tracing apps for COVID-19", *available at SSRN 3609516*, pp.1-7.
- Li, Tianshi, Faklaris, Cori; King, Jennifer; Agarwal, Yuvraj; Dabbish, Laura and Hong, Jason I. (2020) "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps", *arXiv preprint arXiv:2005.11957*, pp.1-23.
- Li, Veronica QT; Ma, Liang and Wu, Xun (2022) "COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia", *Policy and Society*, vol. 41, issue 1, pp. 1-14, <https://doi.org/10.1093/polsoc/puab019>,
- Lintved, Mona Naomi (2021) "COVID-19 Tracing Apps as a Legal Problem: An Investigation of the Norwegian 'Smittestopp' App", *Oslo Law Review*, vol. 8, issue 2, pp.69-87.
- Lucivero, Federica; Hallowell, Nina; Johnson, Stephanie; Prainsack, Barbara; Samuel, Gabrielle and Sharon, Tamar (2020) "COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale", *Bioethical Inquiry*, vol.17, pp.835–839 <https://doi.org/10.1007/s11673-020-10016-9>
- Lueks, Wouter; Benzler, Justus; Bogdanov, Dan; Kirchner, Göran; Lucas, Raquel; Oliveira, Rui; Preneel, Bart; Salathé, Marcel; Troncoso, Carmela and von Wyl, Viktor (2021) "Toward a common performance and effectiveness terminology for digital proximity tracing applications", *Frontiers in digital health*, vol.3, 677929, pp.1-12.
- Malik, Shahnawaz; Mahmood-ul-Hassan and Hussain, Shahzad (2006) "Fiscal decentralisation and economic growth in Pakistan", *The Pakistan Development Review*, pp. 845-854.
- Mancebo Lozano, Esteban (2021) "El estado de bienestar y la nueva gestión de los servicios públicos en España y Latinoamérica: innovación en los servicios sociales y sanitarios tras el Covid-19", *Saber Servir: Revista de la Escuela Nacional de Administración Pública*, vol. 6, pp. 95-121.

- Marhold, Klaus, and Fell, Jan (2022) "Multi-mode standardization under extreme time-pressure—the case of COVID-19 contact-tracing apps", *R&D Management*, vol. 52, n.2, pp. 356-375.
- Márquez Carrasco, Carme and Ortega Ramírez, Juan Antonio (2020) "COVID-19 and the Challenges of Digital Surveillance for Human Rights: Analysis of the App DataCOVID Foreseen in the Ministerial Order SND/29/2020, of March 27th", *Rev. Bioética & Derecho*, vol. 50, pp.205-220.
- Martín Guardado, Sergio (2020) "Real Decreto 463/2020, de 14 de marzo, sobre el estado de alarma", *AIS: Ars Iuris Salmanticensis*, vol. 8, n. 2, pp. 223-228.
- Martínez Martín, Daniel (2021) "Verificación automática del protocolo DP-3T asociado a las aplicaciones COVID-19", Universitat Politècnica de València, <http://hdl.handle.net/10251/173383>, p.39.
- Martínez Martínez, Ricard (2007) "El derecho fundamental a la protección de datos: perspectivas", *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, vol. 5, 4, pp.1-15.
- Mbunge, Elliot (2020) "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol.14, n. 6, pp. 1631-1636.
- McKinney, Scott A.; Landy, Rachel and Wilka, Rachel (2017) "Smart contracts, blockchain, and the next frontier of transactional law", *Wash. JL Tech. & Arts*, vol.13, pp.313-347.
- Mendoza García, María Pilar (2021) "Protección de datos y herramientas tecnológicas para la prevención del Covid-19: análisis a la luz de dos modelos contrapuestos (España vs Emiratos Árabes Unidos)", *Repositorio institucional de la Universidad de Cantabria G1765 Trabajos académicos [692]*, pp.1-38.
- Milne, George R.; Culnan, Mary J. and Greene, Henry (2006): "A longitudinal assessment of online privacy notice readability", *Journal of Public Policy & Marketing*, vol.25, n. 2, pp. 238-249.
- Min-Allah, Nasro; Alahmed, Bashayer Abdullah; Albreek, Elaf Mohammed; Alghamdi, Lina Shabab; Alawad, Doaa Abdullah; Alharbi, Abeer Salem; Al-Akkas, Noor; Musleh, Dhiaa and Alrashed, Saleh (2021) "A survey of COVID-19 contact-tracing apps", *Computers in Biology and Medicine*, vol.137, 104787, pp. 1-11.
- Montesinos Rodrigo, Laura (2022) "Guía para la realización del Privacy Impact Assessment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos", *PhD diss., Universitat Politècnica de València*, pp. 1-72.
- Müller, Regina, Malte Klemmt, Roland Koch, Hans-Jörg Ehni, Tanja Henking, Elisabeth Langmann, Urban Wiesing, and Robert Ranisch. (2024) "'That's just Future Medicine"-a qualitative study on users' experiences of symptom checker apps", *BMC Medical Ethics*, vol. 25, n. 1, pp.17-36.
- Nassimbeni, Guido; Sartor, Marco and Dus, Daiana (2012) "Security risks in service offshoring and outsourcing", *Industrial Management & Data Systems*, vol. 112, n. 3, pp.405-440.
- Newlands, Gemma; Lutz, Christoph; Tamò-Larrieux, Aurelia; Fosch Villaronga, Eduard; Harasgama, Rehana and Scheitlin, Gil (2020) "Innovation under pressure: Implications for data privacy during the Covid-19 pandemic", *Big Data & Society*, vol. 7, n. 2, pp.1-14.
- Nida Bari; Qamar, Usman and Khalid, Ayesha (2021) "Efficient Contact Tracing for pandemics using blockchain", *Informatics in Medicine Unlocked*, vol. 26, p.100742.
- Nieto Garrido, Eva María (2021) "Risks for the fundamental right to the protection of personal data stemming from the COVID-19 sanitary crisis: A Spanish perspective", *Freedom, Security & Justice: European Legal Studies*, n.1, pp. 197-218.

- Nobre, Jéferson Campos; Rodrigues Soares, Laura; Roman Huaytalla, Briggette Olenka; da Silva Júnior, Elvandi and Zambenedetti Granville, Lisandro (2021) "On the Privacy of National Contact Tracing COVID-19 Applications: The Coronavirus-SUS Case", *arXiv preprint arXiv:2108.00921*, <https://arxiv.org/pdf/2108.00921> pp.1-7.
- Nogueira López, Alba, and Doménech Pascual, Gabriel (2020) "Fighting COVID 19 – Legal Powers and Risks", *Spain, VerfBlog*, 2020/3/30, <https://verfassungsblog.de/fighting-covid-19-legal-powers-and-risks-spain/>, DOI: [10.17176/20200331-013028-0](https://doi.org/10.17176/20200331-013028-0)
- O'Leary, Daniel E. (2020) "Evolving Information Systems and Technology Research Issues for COVID-19 and Other Pandemics", *Journal of Organizational Computing and Electronic Commerce*, vol. 30, n.1, pp.1-8.
- Ocheja, Patrick; Cao, Yang; Ding, Shiyao and Yoshikawa, Masatoshi (2020) "Quantifying the Privacy-Utility Trade-offs in COVID-19 Contact Tracing Apps", *arXiv preprint arXiv:2012.13061*, <https://arxiv.org/pdf/2012.13061>, pp.1-14.
- O'Connell, James; Manzar, Abbas; Beecham, Sarah; Buckley, Jim; Chochlov Muslim; Fitzgerald, Brian; Glynn, Liam; Johnson, Kevin; Laffey, John; McNicholas, Bairbre; Nuseibeh, Bashar; O'Callaghan, Michael; O'Keefe, Ian; Razzaq Aabdul; Rekanar, Kaavya; Richardson, Ita; Simpkin, Andrew; Storni, Cristiano; Tsvyatkova, Damyanka; Walsh, Jane; Welsh, Thomas and O'Keefe, Derek (2021) "Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature", *JMIR Mhealth Uhealth*, vol. 9, n.6, e27753, pp.1-23.
- Ogbuefi, Nnubia (2021) "Contact Tracing and Its Approach to Privacy Under Europe and Canada's Privacy Laws", available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4248282, pp.1-59.
- Oliver, Nuria; Lepri, Bruno; Sterly, Harald; Lambiotte, Renaud; Deletaille, Sébastien; De Nadai, Marco; Letouzé, Emmanuel et al. (2020). "Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle", *Science advances*, vol. 6, n.23, eabc0764, pp.1-6.
- Oomen, Isabelle, and Leenes, Ronald (2008) "Privacy risk perceptions and privacy protection strategies", *Policies and research in identity management*, Springer, Boston, pp. 121-138.
- O'Shields, Reggie (2017) "Smart contracts: Legal agreements for the blockchain." *NC Banking Inst.*, vol.21, pp.177-194.
- Osman, Magda; Fenton, Norman Elliot; McLachlan, Scott; Lucas, Peter; Dube, Kudakwashe; Hitman, Graham; Kyrimi, Evangelia; and Neil, Martin (2020) "The thorny problems of Covid-19 Contact Tracing Apps: The need for a holistic approach", *Journal of Behavioral Economics for Policy*, vol.4, n. S, pp. 57-61.
- Owen, Schaefer, G. and Ballantyne, Angela (2022) "Ethics of digital contact tracing wearables", *Journal of Medical Ethics*, vol.48, n. 9, pp.611-615.
- Oyibo, Kiemute; Sahu, Kirti Sundar; Oetomo, Arlene and Morita, Plinio P. (2021) "Factors influencing the adoption of contact tracing applications: Protocol for a systematic review", *JMIR Research Protocols*, vol. 10, n. 6, e28961, pp.1-20. doi: 10.2196/28961 PMID: 33974551 PMCID: 8171387
- Paez, Mauricio and Tobitsch, Kerianne (2017) "The industrial internet of things: Risks, liabilities, and emerging legal issues", *NYL Sch. L. Rev.*, vol.62, pp. 217-247.
- Paine, Carina; Reips, Ulf-Dietrich; Stieger, Stefan; Joinson, Adam and Buchanan, Tom (2007) "Internet users' perceptions of 'privacy concerns and 'privacy actions", *International Journal of Human-Computer Studies*, vol.65, n.6, pp. 526-536,
- Pazos Vidal, Serafín (2021) "La dimensión territorial de la pandemia", *Informe sobre la Democracia en España 2020: El Año de la Pandemia*, pp. 171-188.

- Peguera Poch, Miquel (2019) "The right to be forgotten in the European Union", *The Oxford Handbook of Online Intermediary Liability (OUP, 2019 Forthcoming)*, pp.1-16.
- Politou, Eugenia; Alepis, Efthimios and Patsakis, Constantinos (2018) "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions", *Journal of cybersecurity*, vol. 4, n. 1, pp. 1-20.
- Politou, Eugenia; Michota, Alexandra; Alepis, Efthimios; Pocs, Matthias and Patsakis, Constantinos (2018) "Backups and the right to be forgotten in the GDPR: An uneasy relationship", *Computer Law & Security Review*, vol. 34, n. 6 pp.1247-1257.
- Ponce, Aida (2020) "COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim", *ETUI Research Paper-Policy Brief*, vol. 5, p.3.
- Pop, Claudia Daniela; Antal, Marcel; Cioara, Tudor; Anghel, Ionut and Salomie, Ioan (2020) "Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy", *Sensors*, vol.20, n. 19, pp. 5678.
- Prabhakar, Salil; Pankanti, Sharath and Jain, Anil K. (2003) "Biometric recognition: Security and privacy concerns", *IEEE security & privacy*, vol. 1, n. 2, pp. 33-42.
- Presno Linera, Miguel Ángel (2020) "Estado de alarma por coronavirus y protección jurídica de los grupos vulnerables", *Revista Derecho Público*, n. 94, Dossî Especial-Covid-19, pp. 15-34.
- Quiroga Sánchez del Campo, María (2022) "El derecho a la protección de datos personales frente a emergencias sanitarias" *Universidad Pontificia Comillas, Facultad de Derecho*, pp. 1-46.
- Raab, Charles D. (1998) "The distribution of privacy risks: Who needs protection?", *The information society*, vol.14, n. 4, pp.263-274.
- Raab, Charles D. (2020) "Information privacy, impact assessment, and the place of ethics", *Computer Law & Security Review*, vol.37, 105404, pp. 1-16.
- Rahate, Sachin W., and Shaikh, M. Zafar (2016) "Geo-fencing infrastructure: Location based service", *International Research Journal of Engineering and Technology*, vol. 3, n. 11, p.1095-1098.
- Raman, Raghu; Achuthan, Krishnashree; Vinuesa, Ricardo and Nedungadi, Prema (2021) "COVIDTAS COVID-19 Tracing App Scale-An Evaluation Framework", *Sustainability*, vol.13, n. 5, pp. 1-19.
- Raskar, Ramesh; Dhillon, Ranu; Kapa, Suraj; Pahwa, Deepti; Falgas, Renaud; Sinha, Lagnojita; Prasad, Aarathi et al. (2020) "Comparing manual contact tracing and digital contact advice." *arXiv preprint arXiv:2008.07325* <https://arxiv.org/pdf/2008.07325>, pp.1-9.
- Ravizza, Alice; Sternini, Federico; Molinari, Filippo; Santoro, Eugenio and Cabitza, Federico (2021) "A proposal for COVID-19 applications enabling extensive epidemiological studies", *Procedia computer science*, vol.181, pp. 589-596.
- Recio, Miguel; Albiñana, CMS; and Suárez de Lezo (European Audiovisual Observatory) (2019) "Spain Goes Further Than The GDPR When Adapting Its Data Protection Law", *IRIS Legal Observations of the European Audiovisual Observatory*, available at <https://merlin.obs.coe.int/article/8502> (accessed on 15 July 2024)
- Reichert, Leonie; Brack, Samuel and Scheuermann, Björn (2020) "Privacy-preserving contact tracing of COVID-19 patients", *Cryptology ePrint Archive*, pp.1-2.
- Rivas Castillo, David (2020) "Protección De Datos: Evolución, Actualidad, Análisis Y La Influencia Del Covid-19", *Universidad de Jaén*, <https://hdl.handle.net/10953.1/12895>, pp.1-38.

- Rodríguez Ayuso, Juan Francisco (2020) "Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia", *Revista de bioética y Derecho*, vol. 50, pp.353-368.
- Rodríguez Prieto, Rafael (2020) "Consecuencias de la STC 76/2019, de 22 de mayo en la privacidad y uso de apps para el control de la COVID. El caso de Radar COVID", *Cuadernos electrónicos de filosofía del derecho*, vol. 43, pp. 189-219.
- Rodríguez, Jorge P.; Aleta, Alberto and Moreno, Yamir (2023) "Digital cities and the spread of COVID-19: Characterizing the impact of non-pharmaceutical interventions in five cities in Spain", *Frontiers in Public Health*, vol. 11, 1122230, pp.78-88.
- Rodríguez, Pablo; Graña, Santiago; Alvarez-León, Eva Elisa; Battaglini, Manuela; Darias, Francisco Javier; Hernán, Miguel A.; López, Raquel et al. (2021) "A population-based controlled experiment assessing the epidemiological impact of digital contact tracing", *Nature Communications*, vol.12, n. 1, pp. 1-6.
- Roig Batalla, Antoni (2021) "Garantías frente a las aplicaciones de rastreo de contagios en situaciones de pandemia", *Teoría y realidad constitucional*, vol.48, pp. 527-542.
- Rubí Puig, Antoni and Herrerías Castro, Laura (2022) "Radar COVID» and protection of personal data. An analysis of the disciplinary procedures of the Spanish Data Protection Agency", *InDret*, vol. 4, pp. 249-280.
- Sales, Bruce D., and Krauss, Daniel A. (2015) "The psychology of law: Human behavior, legal institutions, and law", *American Psychological Association*, available at <http://www.jstor.org/stable/j.ctv1chs58t>
- Samuel, Gabby; Roberts, Stephen L.; Fiske, Amelia; Lucivero Federica; McLennan, Stuart; Phillips, Amicia; Hayes, Sarah and Johnson, Suzanne B. (2022) "COVID-19 contact tracing apps: UK public perceptions", *Critical Public Health*, vol. 32, n.1, pp.31-43, DOI: 10.1080/09581596.2021.1909707.
- Sánchez Ferriz, Remedio (2020) "Reflexiones constitucionales desde el confinamiento", en *Actualidad Jurídica Iberoamericana*, núm. 12 bis, pp. 16-23.
- Sanz Guedán, Sara (2021) "Geolocalización de las personas físicas en el contexto de la pandemia por la COVID 19." Universidad de Valladolid. Facultad de Ciencias Sociales, Jurídicas y de la Comunicación, pp.1-67, <https://uvadoc.uva.es/handle/10324/48151>
- Scantamburlo, Teresa; Cortés, Atia; Dewitte, Pierre; Van der Eycken, Daphné; De Wolf, Ralf and Martens, Marijn "Covid-19 and tracing methodologies: A lesson for the future society", *Health Technol.*, Vol. 11, <https://doi.org/10.1007/s12553-021-00575-1>, pp.1051–1061.
- Scassa, Teresa; Millar, Jason and Bronson, Kelly (2020) "Privacy, Ethics, and Contact-tracing Apps", in Colleen M. Flood, Vanessa MacDonnell, Jane Philpott, Sophie Thériault and Sridhar Venkatapuram, eds., *Vulnerable: The Law and Policy of COVID-19*, University of Ottawa Press, pp.1-8, online: <https://ruor.uottawa.ca/handle/10393/40726>.
- Schaar, Peter (2010) "Privacy by Design", *IDIS*, vol.3, pp. 267–274.
- Scrivano, Noemi; Gulino, Rosario Alfio and Giansanti, Daniele (2022) "Digital Contact Tracing and COVID-19: Design, Deployment, and Current Use in Italy", *Healthcare* 2022, vol.10, 67, pp.1-11. <https://doi.org/10.3390/healthcare10010067>.
- Seinen, Wouter; Walter, Andre and van Grondelle, Sari (2018) "Compatibility as a mechanism for responsible further processing of personal data", *Annual Privacy Forum*, Springer, pp. 153-171.

- Senarath, Awanthika and Arachchilage, Nalin Asanka Gamagedara (2018) "Understanding software developers' approach towards implementing data minimization", *arXiv preprint* arXiv:1808.01479 <https://arxiv.org/pdf/1808.01479>, pp.1-4.
- Servet, Vicente Magro (2020) "El reproche penal a los actos de desobediencia a agentes de la autoridad en el período de Estado de Alarma por el Coronavirus." *Diario la ley*, vol.9606, n. 2, pp.1-15.
- Shahroz, Muhammad; Ahmad, Farooq; Younis, Muhammad Shahzad; Ahmad, Nadeem; Boulos, Maged N. Kamel; Vinuesa, Ricardo and Qadir, Junaid (2021) "COVID-19 digital contact tracing applications and techniques: A review post initial deployments", *Transportation Engineering*, vol.5, 100072, pp.1-9.
- Sharma, Shavneet; Singh, Gurmeet; Sharma, Rashmini; Jones, Paul; Kraus, Sascha and Dwivedi, Yogesh K. (2020) "Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps", *IEEE Transactions on Engineering Management*, pp.1-17.
- Shoji, Masahiro; Cato, Susumu; Ito, Asei; Iida, Takashi; Ishida, Kenji; Katsumata, Hiroto and McElwain, Kenneth Mori (2022) "Mobile health technology as a solution to self-control problems: The behavioral impact of COVID-19 contact tracing apps in Japan", *Social Science & Medicine*, vol.306, p.115142.
- Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2021) "Effectiveness modeling of digital contact-tracing solutions for tackling the COVID-19 pandemic", *The Journal of Navigation*, vol.74, n. 4, pp. 853-886.
- Shukla, Manish; Lodha, Sachin; Shroff, Gautam; Rajan, M.A and Raskar, Ramesh (2020) "Privacy guidelines for contact tracing applications", *arXiv preprint* arXiv:2004.13328, <https://arxiv.org/pdf/2004.13328> , pp.1-10.
- Simko, Lucy; Calo, Ryan; Roesner, Franziska and Kohno, Tadayoshi (2020). "COVID-19 contact tracing and privacy: studying opinion and preferences", *arXiv preprint* arXiv:2005.06056 <https://arxiv.org/pdf/2005.06056>, pp.1-32.
- Simón Castellano, Pere (2013) "A Test for Data Protection Rights Effectiveness: Charting the Future of the 'Right to Be Forgotten' Under European Law", *Columbia Journal of European Law Online*, pp.1-5.
- Singh, Hanson John Leon; Couch, Danielle and Yap, Kevin (2020) "Mobile health apps that help with COVID-19 management: scoping review", *JMIR nursing*, vol. 3, n. 1, e20596, pp.1-16.
- Sowmiya B.; Abhijith VS.; Sudersan, S; Sakthi Jaya Sundar, R; Thangavel M; Varalakshmi P. A. (2021) "Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19", *SN Comput Sci.*, vol.2, n.3, pp.1-11, doi: 10.1007/s42979-021-00520-z.
- Splinter, Bas; Saadah, Nicholas H.; Chavannes, Niels H.; Kieffe-de Jong, Jessica C. and Aardoom, Jiska J. (2022) "Optimizing the Acceptability, Adherence, and Inclusiveness of the COVID Radar Surveillance App: Qualitative Study Using Focus Groups, Thematic Content Analysis, and Usability Testing", *JMIR Formative Research*, vol. 6, n. 9, e36003, pp.1-15.
- Stalla-Bourdillon, Sophie; Thuermer, Gefion; Walker, Johanna; Carmichael, Laura and Simperl, Elena (2020) "Data protection by design: building the foundations of trustworthy data sharing", *Data & Policy*, vol. 2, pp. e4-5.
- Tedeschi, Pietro; Bakiras, Spiridon and Di Pietro, Roberto (2021) "IoTrace: a flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing", *IEEE Communications Magazine*, vol.59, n. 6, pp. 82-88.
- Tene, Omer, and Polonetsky, Jules (2011) "Privacy in the age of big data: a time for big decisions", *Stan. L. Rev. Online*, vol.64, pp.63-69.

- Toch, Eran; Wang, Yang and Cranor, Lorrie Faith (2012) "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems", *User Modeling and User-Adapted Interaction*, vol.22, n.1, pp.203-220.
- Touzani, Rajae; Schultz, Emilien; Holmes, Seth M.; Vandentorren, Stéphanie; Arwidson, Pierre; Guillemain, Francis; Rey, Dominique; Rouquette, Alexandra; Bouhnik, Anne-Déborah and Mancini, Julien (2021) "Early acceptability of a mobile app for contact tracing during the COVID-19 pandemic in France: National web-based survey", *JMIR mHealth and uHealth* vol. 9, n. 7, e27768, pp.1-13,
- Tran, Cong Duc and Nguyen, Tin Trung (2021) "Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps", *Technology in Society*, vol. 67,101755, pp.1-11. doi: 10.1016/j.techsoc.2021.101755. Epub 2021 Sep 21. PMID: 34566204; PMCID: PMC8454194.
- Trang, Simon; Trenz, Manuel; Weiger, Welf H.; Tarafdar, Monideepa; Cheung, Christy M.K. (2020) "One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps", *European Journal of Information Systems*, vol. 29, n.4, pp. 415-428, DOI: 10.1080/0960085X.2020.1784046.
- Trivedi, Ameer and Vasisht, Deepak (2020) "Digital contact tracing: technologies, shortcomings, and the path forward", *ACM SIGCOMM Computer Communication Review*, vol.50, n. 4, pp. 75-81.
- Trivedi, Ameer; Zakaria, Camellia; Balan, Rajesh; Becker, Ann; Corey, George and Shenoy, Prashant (2021) "Wifitrace: Network-based contact tracing for infectious diseases using passive wifi sensing", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, n. 1, pp.1-26
- Trotoch, Rachel L. (2020). "A comparative analysis of data privacy impacted by COVID-19 contact tracing in the European union, the United States, and Israel: sacrificing civil liberties for a public health emergency", *ILSA J. Int'l & Comp. L.*, vol. 27, pp.55-76.
- Truong, Nguyen Binh; Sun, Kai; Lee, Gyu Myoung and Guo, Yike (2019) "GDPR-compliant personal data management: A blockchain-based solution", *IEEE Transactions on Information Forensics and Security*, vol.15, pp. 1746-1761
- Ussai, Silvia; Pistis, Marco; Missoni, Eduardo; Formenti, Beatrice; Armocida, Benedetta; Pedrazzi, Tatiana; Castelli, Francesco; Monasta, Lorenzo; Lauria, Baldassare and Mariani, Ilaria (2022) "'Immuni' and the National Health System: Lessons Learnt from the COVID-19 Digital Contact Tracing in Italy", *International Journal of Environmental Research and Public Health*, vol.19, n. 12, 7529, pp.1-7.
- Utrilla, Dolores; García-Muñoz, Manuel Antonio and Pareja Sánchez, Teresa (2021) "Spain: Legal Response to Covid-19", in Jeff King and Octávio LM Ferraz et al (eds), *The Oxford Compendium of National Legal Responses to Covid-19* (OUP 2021). pp.1-34, doi: 10.1093/law-occ19/e10.013.10
- Vaishya, Raju; Javaid, Mohd; Khan, Ibrahim Haleem and Haleem, Abid (2020) "Artificial Intelligence (AI) applications for COVID-19 pandemic", *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, n. 4, pp. 337-339.
- Valero Torrijos, Julián and Cerdá Meseguer, Juan Ignacio (2020) "Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del COVID-19", *EUNOMÍA. Revista en Cultura de la Legalidad*, vol.19, pp. 103-126.
- van Dijk, William J.; Saadah, Nicholas H.; Numans, Mattijs E.; Aardoom, Jiska J.; Bonten, Tobias N.; Brandjes, Menno; Brust, Michelle et al. (2021) "COVID RADAR app: description and validation of population surveillance of symptoms and behavior in relation to COVID-19", *Plos one*, vol. 16, n. 6, e0253566, pp.1-18. <https://doi.org/10.1371/journal.pone.0253566>
- Van Kolschooten, Hannah, and de Ruijter, Anniek (2020) "COVID-19 and privacy in the European Union: A legal perspective on contact tracing", *Contemporary Security Policy*, vol. 41, n. 3, pp. 478-491.

- Van Zoonen, Liesbet (2016) "Privacy concerns in smart cities", *Government Information Quarterly*, vol. 33, n. 3, pp. 472-480.
- Vaudenay, Serge (2020) "Analysis of DP3T-between scylla and charybdis", *Cryptology ePrint Archive*, Paper 2020/399, <https://ia.cr/2020/399>, pp.1-12.
- Vaudenay, Serge (2020) "Centralized or decentralized? The contact tracing dilemma", *Cryptology ePrint Archive*, pp. 1-31.
- Veale, Michael (2020) "Sovereignty, Privacy, and Contact Tracing Protocols", *Meatspace Press*, pp.35-39.
- Veale, Michael; Binns, Reuben and Ausloos, Jef (2018) "When data protection by design and data subject rights clash", *International Data Privacy Law*, vol. 8, n. 2, pp. 105-123.
- Velicia-Martin, Felix; Cabrera-Sanchez, Juan-Pedro; Gil-Cordero, Eloy and Palos-Sanchez, Pedro R. (2021) "Researching COVID-19 tracing app acceptance: incorporating theory from the technological acceptance model", *PeerJ Computer Science*, vol. 7, p. e316, pp.1-20.
- Vergallo, Ginaluca Montanari; Zaami, Simona; Bruti, Valerio; Signore, Fabrizio and Marinelli, Enrico (2021) "The COVID-19 pandemic and contact tracing technologies, between upholding the right to health and personal data protection", *European Review for Medical and Pharmacological Sciences*, vol. 25, n. 5, pp.2449-2456.
- Vicente Díaz, Matilde and Callejo Carrión, Soraya (2021) "On alarms, geolocations and rights: Regarding a regulation that is more than dangerous for fundamental rights", *CEFLegal. Practical Law Review*, pp.109-142.
- Villaplana Jiménez, Francisco Ramón (2021) "Recursos digitales de colaboración y de seguridad pública. Mejorando la autoprotección ciudadana", *RIPS: Revista de Investigaciones Políticas y Sociológicas*, vol. 20, n.2, pp. 1-18, <https://doi.org/10.15304/rips.20.2.7989>.
- Vinuesa, Ricardo; Theodorou, Andreas; Battaglini, Manuela and Dignum, Virginia (2020) "A socio-technical framework for digital contact tracing", *Results in Engineering*, vol.8, 100163, pp.1-4.
- Vuokko, Riikka; Saranto, Kaija and Palojoki, Sari (2021) "Features of COVID-19 applications and their impact on contact tracing: results of preliminary review", *Finnish Journal of eHealth and eWelfare*, vol.13, n. 4, pp.347-359.
- Walrave, Michel; Waeterloos, Cato and Ponnet, Koen (1 Sept. 2020) "Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach", *JMIR Public Health Surve ill.*, vol.6, n.3, e20572, pp.1-10, doi: 10.2196/20572. PMID: 32755882; PMCID: PMC7470174.
- Watson, Jason; Richter Lipford, Heather and Besmer, Andrew (2015) "Mapping user preference to privacy default settings", *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 22, n. 6, pp. 1-20.
- Weiß, Jan-Patrick; Esdar, Moritz and Hübner, Ursula (2021) "Analyzing the essential attributes of nationally issued COVID-19 contact tracing apps: Open-source intelligence approach and content analysis", *JMIR mHealth and uHealth* 9, n. 3, e27232, pp.1-16, doi: [10.2196/27232](https://doi.org/10.2196/27232) PMID: [33724920](https://pubmed.ncbi.nlm.nih.gov/33724920/) PMCID: [8006898](https://pubmed.ncbi.nlm.nih.gov/8006898/).
- Weitze, Tobias; Barros, Henrique and Byun, Hyunji (2020) "Contact Tracing Apps for COVID-19 An Overview of the European Region", *The Association of Schools of Public Health in the European Region (ASPHER)*, pp.1-21.
- White, Lucie and van Basshuysen, Philippe (2021) "Privacy versus public health? A reassessment of centralised and decentralised digital contact tracing", *Science and Engineering Ethics*, vol. 27, n. 2, pp. 23-36, <https://doi.org/10.1007/s11948-021-00301-0>
- Williams, Simon N.; Armitage, Christopher J.; Tampe, Tova and Dienes, Kimberly (2021) "Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study", *Health Expect*, vol. 24, n.2, pp. 377-385.

- Willis, Lauren E. (2014) "Why not privacy by default", *Berkeley Tech. LJ*, vol. 29, p. 61-134.
- Wright, David (2013) "Making privacy impact assessment more effective", *The Information Society*, vol.29, n. 5, pp. 307-315.
- Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart, Paul (2011) "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, vol. 12, n. 1, pp. 798-824.
- Youn, Seounmi (2009) "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents", *Journal of Consumer affairs*, vol.43, n. 3, pp.389-418.
- Zafir, Gabriela (2014) "Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law", *Reloading Data Protection*, Springer, Dordrecht, pp. 237-257.
- Zarsky, Tal Z. (2016) "Incompatible: The GDPR in the age of big data", *Seton Hall L. Rev.*, vol.47, pp. 995-1020.
- Zeng, Kylie; Bernardo, Stephanie N. and Havins, Weldon E. (2020) "The use of digital tools to mitigate the COVID-19 pandemic: comparative retrospective study of six countries", *JMIR public health and surveillance*, vol. 6, n. 4, e24598, pp.1-15, URL: <http://publichealth.jmir.org/2020/4/e24598/> doi: 10.2196/24598 PMID: 33302255.
- Zhang, Melvyn; Chow, Aloysius and Smith, Helen (2020) "COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies", *J Med Internet Res*, vol. 22, n.12,e21572, pp.1-6, doi: [10.2196/21572](https://doi.org/10.2196/21572) PMID: [33170798](https://pubmed.ncbi.nlm.nih.gov/33170798/) PMCID: [7717894](https://pubmed.ncbi.nlm.nih.gov/7717894/).
- Zhou, Jiapeng; Feng, Yuxiang; Wang, Zhenyu and Guo, Danyi (2021) "Using secure multi-party computation to protect privacy on a permissioned blockchain", *Sensors*, vol. 21, n. 4,1540, pp. 1-17.
- Zwitter, Andrej and Gstrein, Oskar Josef (2020) "Big data, privacy and COVID-19—learning from humanitarian expertise in data protection", *Journal of International Humanitarian Action*, vol. 5, n. 1, pp. 1-7.

Published Conference Papers:

- Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira et al. (2020) "Mind the gap: Security & privacy risks of contact tracing apps", *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, pp. 458-467.
- Bellekens, Xavier; Hamilton, Andrew; Seeam, Preetila; Nieradzinska, Kamila; Franssen, Quentin and Seeam, Amar (2016) "Pervasive eHealth services a security and privacy risk awareness survey", *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pp. 1-4.
- Bhatia, Jaspreet; Breaux, Travis D.; Friedberg, Liora; Hibshi, Hanan and Smullen, Daniel (2016) "Privacy risk in cybersecurity data sharing", *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 57-64
- Daudén-Esmel, Cristòfol; Castellà-Roca, Jordi; Viejo, Alexandre and Domingo-Ferrer, Josep (2021) "Lightweight blockchain-based platform for gdpr-compliant personal data management", *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pp. 68-73.
- Duarte, Tatiana (2022) "Google and Apple Exposure Notifications System: Exposure Notifications or Notified Exposures?", *Annual Privacy Forum*, Springer, Cham, pp. 99-118.

- Evans, Geoffrey; Bostrom, Ann; Johnston, Richard B.; Fisher, Barbara Loe and Stoto, Michael A. (1997) "Risk communication and vaccination: summary of a workshop", Institute of Medicine (US) Vaccine Safety Forum. Risk Communication and Vaccination: Summary of a Workshop. Washington (DC): National Academies Press (US); 1997. PMID: 25121223.
- Ezzaouia, Imane, and Bulchand-Gidumal, Jacques (2021) "A Model to Predict Users' Intentions to Adopt Contact-Tracing Apps for Prevention from COVID-19", *Information and Communication Technologies in Tourism 2021: Proceedings of the ENTER 2021 eTourism Conference, January 19–22, 2021*, Cham: Springer International Publishing, pp. 543-548.
- Freudiger, Julien; Shokri, Reza and Hubaux, Jean-Pierre (2011) "Evaluating the privacy risk of location-based services", *International conference on financial cryptography and data security*, Springer, Berlin, Heidelberg, pp. 31-46.
- Friedewald, Michael; Schiering, Ina; Martin, Nicholas; and Hallinan, Dara (2022) "Data Protection Impact Assessments in Practice", European Symposium on Computer Security, *ESORICS 2021 International Workshops*. Lecture Notes in Computer Science, vol 13106. Springer, Cham. https://doi.org/10.1007/978-3-030-95484-0_25, pp. 424-443.
- Galdón-Clavell, Gemma; Zamorano, Mariano Martín; Castillo, Carlos; Smith, Oliver and Matic, Aleksandar (2020) "Auditing algorithms: On lessons learned and the risks of data minimization", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 265-271.
- Hong, Jason I.; Jennifer D. Ng; Lederer, Scott and Landay, James A. (2004) "Privacy risk models for designing privacy-sensitive ubiquitous computing systems", *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pp. 91-100.
- Huth, Dominik and Matthes, Florian (2019) "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements", *Americas Conference on Information Systems*, pp.1-10.
- Jo Pesch, Paulina; Dimitrova, Diana and Boehm, Franziska (2022) "Data Protection and Machine-Learning-Supported Decision-Making at the EU Border: ETIAS Profiling Under Scrutiny", *Annual Privacy Forum*, Springer, Cham, pp. 50-72.
- Kamocki, Paweł, and Siegert, Ingo (2022) "Pseudonymisation of speech data as an alternative approach to GDPR compliance", *Proceedings of the LREC 2022 Joint Workshop on Legal and Ethical Issues in Human Language Technologies and Multilingual De-Identification of Sensitive Language Resources (LEGAL-MDLR 2022)*. Marseille, 20 June 2022, European Language Resources Association (ELRA), pp. 17-21.
- Kasirzadeh, Atoosa, and Clifford, Damian (2021) "Fairness and Data Protection Impact Assessments", *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 146-153
- Martin, Yod-Samuel, and Kung, Antonio "Methods and tools for GDPR compliance through privacy and data protection engineering", 2018 IEEE European symposium on security and privacy workshops (EuroS&PW), IEEE, 2018. pp. 108-111.
- Nakamura, Toru; Kiyomoto, Shinsaku; Welderufael B. Tesfay, and Serna, Jetzabel (2016) "Personalised privacy by default preferences-experiment and analysis", *International Conference on Information Systems Security and Privacy*, vol. 2, SCITEPRESS, pp. 53-62.
- Perera, Charith; McCormick, Ciaran; Bandara, Arosha K.; Price, Blaine A. and Nuseibeh, Bashar (2016) "Privacy-by-design framework for assessing internet of things applications and platforms", *Proceedings of the 6th International Conference on the Internet of Things*, pp. 83-92
- Rehak, Rainer; Kühne, Christian R. and Bock, Kirsten (2022) "Analysis and Constructive Criticism of the Official Data Protection Impact Assessment of the German Corona-Warn-App", *Annual Privacy Forum*, Springer, Cham, pp. 119-134.
- Shubina, Viktoriia; Ometov, Aleksandr; Basiri, Anahid and Lohan, Elena Simona (2020) "October. Technical Perspectives of Contact-Tracing Applications on Wearables for

- COVID-19 Control”, 2020 12th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 229-235.
- Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth and Ranasinghe, Damith C. (2020) "VenueTrace: a privacy-by-design COVID-19 digital contact tracing solution", *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pp. 790-791.
 - Sun, Ruoxi; Wang, Wei; Xue, Minhui; Tyson, Gareth; Camtepe, Seyit and Ranasinghe, Damith C. (2021) "An empirical assessment of global COVID-19 contact tracing applications", *IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, pp. 1085-1097.
 - Troncoso, Carmela ; Payer, Mathias; Hubaux, Jean-Pierre ; Salathé, Marcel; Larus, James R. ; Lueks, Wouter ; Stadler, Tanja et al. (2020) "Decentralized Privacy-Preserving Proximity Tracing." (2020) "Decentralized Privacy-Preserving Proximity Tracing", *IEEE Data Engineering Bulletin*, vol. 43, n.2, pp. 36-66.
 - Udoh, Emmanuel Sebastian and Alkharashi, Abdulwahab (2016) "Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students", *2016 Future Technologies Conference (FTC)*, pp. 926-931.
 - Vemou, Konstantina and Karyda, Maria (2018) "An Evaluation Framework for Privacy Impact Assessment Methods", *MCIS 2018 Proceedings*, n.5, pp.1-10, <https://aisel.aisnet.org/mcis2018/>.
 - Ventrella, Emanuele (2020) "Privacy in emergency circumstances: data protection and the COVID-19 pandemic", *ERA Forum*, n.21, pp. 379–393, <https://doi.org/10.1007/s12027-020-00629-3>
 - Wairimu, Samuel, and Momen, Nurul (2021) "Privacy analysis of covid-19 contact tracing apps in the EU", *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings*, n. 25, Springer International Publishing, pp. 213-228.
 - Wang, Na; Wisniewski, Pamela; Xu, Heng and Grossklags, Jens (2014) "Designing the default privacy settings for Facebook applications", *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing*, pp. 249-252.
 - Welsh, Thomas; Rekanar, Kaavya; Abbas, Manzar; Chochlov, Muslim; Fitzgerald, Brian; Glynn, Liam; Johnson, Kevin et al. (2020) "Towards a taxonomy for evaluating societal concerns of contact tracing apps", *2020 7th International Conference on Behavioural and Social Computing (BESC), IEEE*, pp. 1-6.
 - Wen, Haohuang; Zhao, Qingchuan; Lin, Zhiqiang; Xuan, Dong and Shroff, Ness (2020) "A study of the privacy of Covid-19 contact tracing apps", *Security and Privacy in Communication Networks: 16th EAI International Conference, SecureComm 2020, Washington, DC, USA, October 21-23, 2020, Proceedings, Part I*, n.16, Springer International Publishing, pp. 297-317.

Reports, communications, and guidance from data protection authorities and other relevant local and European Union authorities:

- AEPD (2019) The Duty To Inform And Other Accountability Measures For Mobile Devices, available at: <https://www.aepd.es/documento/nota-tecnica-apps-moviles-en.pdf> (accessed on 15 February 2024).
- AEPD (2020) Recommendations to protect personal data in situations of mobility and telecommuting guidance <https://www.aepd.es/documento/nota-tecnica-protoger-datos-teletrabajo-en.pdf> (accessed on 15 February 2024).
- AEPD (2020) Report From The State Legal Service (Detached Department of the SIs at the Spanish DPA) On Processing Activities Relating to the Obligation For Controllers From Private Companies And Public Administrations to Report On Workers Suffering From Covid-19 available at: <https://www.aepd.es/documento/2020-0017-en.pdf> (accessed on 23 June 2024).

- AEPD (2020), Notice on Corona Virus Self-Assessment Apps and Websites <https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/aepds-notice-on-coronavirus-self-assessment-apps-and-websites> (accessed on 23 June 2024).
- AEPD (2021) Guide on Use of Cookies available at: <https://www.aepd.es/documento/guia-cookies-en.pdf> (accessed on 15 February 2024).
- AEPD (2021) Risk management and impact assessment in processing activities available at: <https://www.aepd.es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf> (accessed on 23 June 2024).
- AEPD, (2020) Informe 017/2020 on the Treatment of Data Derived from the Present COVID-19 Virus Situation (Mar. 12, 2020), <https://perma.cc/Z8GA-655Y>. (accessed on 23 June 2024).
- AEPD, Guía para el cumplimiento del deber de informar <https://www.aepd.es/documento/guia-modelo-clausula-informativa.pdf> (accessed on 15 February 2024).
- AEPD, Guía sobre el uso de videocámaras para seguridad y otras finalidades <https://www.aepd.es/documento/guia-videovigilancia.pdf> (accessed on 15 February 2024)
- Article 29 Data Protection Working Party (2013), Opinion 03/2013, Opinion on Purpose Limitation https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (accessed on 16 October 2023).
- Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymization Techniques. Adopted on 10 April 2014 (wp216). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (accessed on 23 June 2024).
- Article 29 Data Protection Working Party, (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/items/611236> (accessed on 23 June 2024).
- Article 29 Working Party (2018) Guidelines on Personal data breach notifications under Regulation 2016 <https://ec.europa.eu/newsroom/article29/items/612052/en> (accessed on 23 June 2024).
- Article 29 Working Party, (2018) Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017. Last Revised and Adopted on 10 April 2018. <https://ec.europa.eu/newsroom/article29/items/623051/en> (accessed on 23 June 2024).
- Article 29 Working Party, (2018) Guidelines on Transparency under Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/items/622227/en> (accessed on 23 June 2024).
- Article 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01), protection of personal data https://www.europarl.europa.eu/charter/pdf/text_en.pdf .
- Charter of Fundamental Rights of the European Union, “Right to respect for private and family life, home and correspondence” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> .
- Civil Liberties Organisations Across the European Union (2020) “EU 2020: Demanding On Democracy Country & Trend Reports on Democratic Records, Spain” https://dg4n3btxmr8c9.cloudfront.net/files/6th9cw/Liberties_RoL_report_2021_SE.pdf (accessed on 23 June 2024).
- CNIL (French Data Protection Authority) Guideline, (2018) “Security of Personal Data,” https://www.cnil.fr/sites/default/files/atoms/files/guide_security-personal-data_en.pdf (accessed on 23 June 2024).
- Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (OJ L 114 14.04.2020, ELI: <http://data.europa.eu/eli/reco/2020/518/oj>) (accessed on 23 June 2024).
- Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: <https://eur->

- [lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)) (accessed on 23 June 2024).
- Communication From The Commission To The European Parliament And The Council Exchanging And Protecting Personal Data In A Globalised World <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN> (accessed on 23 June 2024).
 - Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A European Strategy For Data Available At: <https://Eur-Lex.Europa.Eu/Legal-Content/En/Txt/?Uri=Celex%3a52020dc0066> (accessed on 23 June 2024).
 - Considerations for contact tracing during the monkeypox outbreak in Europe, 2022, 28 June 2022, European Centre for Disease Prevention and Control.
 - Contact Tracing with Mobile Applications, Tech Dispatch, Issue 1, 2020 https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en (accessed on 23 June 2024).
 - Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU* available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_869 (accessed on 23 June 2024).
 - Council of Europe, Contact Tracing Apps available at <https://www.coe.int/en/web/data-protection/contact-tracing-apps> (accessed on 23 June 2024).
 - Council of Europe, Covid 19 and Data Protection <https://www.coe.int/en/web/data-protection/covid-19-data-protection> (accessed on 23 June 2024).
 - Data Protection Website, Data Protection Impact Assessments <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=The%20DPIA%20should%20be%20carried,design%20of%20the%20processing%20operation>. (accessed on 23 June 2024).
 - ECHR Guide on Article 8 of the European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/guide_art_8_eng (accessed on 23 June 2024)
 - EDPB (2018) Guidelines on transparency under Regulation 2016/679, https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en (accessed on 12 February 2024).
 - EDPB (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (accessed on 12 February 2024).
 - EDPB (2019) Guidelines 4/2019 regarding Article 25 Data Protection by Design and Default https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (accessed on 12 February 2024).
 - EDPB (2020), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed on 23 June 2024).
 - EDPB (2022) Guidelines 9/2022 on personal data breach notification under GDPR https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en (accessed on 12 February 2024).
 - EDPB (2023) Guidelines 01/2022 on data subject rights- Right of access, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (accessed on 23 June 2024).
 - EDPB Website, Respect Individuals Rights https://edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en (accessed on 23 June 2024).

- EDPB, (2020) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak” available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en (accessed on 12 February 2024).
- EDPB, (2020) Guidelines 05/2020 on consent under Regulation 2016/679 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (accessed on 23 June 2024).
- EDPB, (2020) Guidelines 10/2020 on Restrictions under Art. 23 GDPR https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-102020-restrictions-under-article-23_en (accessed on 12 February 2024).
- EDPB, (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (accessed on 12 February 2024).
- EDPB, (2021) Guidelines 07/2020 on the concepts of controller and processor in the GDPR, available at: https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf (accessed on 23 June 2024).
- EDPB, (2021) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01 available at: https://www.edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf (accessed on 12 February 2024).
- EDPS comments on the Commission draft implementing decision amending Implementing Decision 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic.
- EDPS Opinion on the European Commission's Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)” available at: https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf (accessed on 15 February 2024).
- EDPS Opinion on the proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation available at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-council-directive_en (accessed on 23 June 2024).
- EDPS Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis, 2 February 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-manual-contact-tracing-eu_en (accessed on 23 June 2024).
- EDPS, (2020) TechDispatch #1/2020: Contact Tracing with Mobile Applications Available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en (accessed on 23 June 2024).
- EDPS, (2022) TechDispatch, Federated Social Media Platforms https://edps.europa.eu/system/files/2022-07/22-07-26_techdispatch-1-2022-federated-social-media-platforms_en.pdf (accessed on 23 June 2024).
- EDPS, “Checklist 3: What is required in a processing agreement?” available at: https://www.edps.europa.eu/sites/default/files/publication/19-09-27_checklist_3requirements_processing_en.pdf (accessed on 15 February 2024).
- eHealth Network (2020), Interoperability guidelines for approved contact tracing mobile applications in the EU https://health.ec.europa.eu/system/files/2020-05/contacttracing_mobileapps_guidelines_en_2.pdf (accessed on 23 June 2024).

- eHealth Network (2020), Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States 15 April 2020 https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf (accessed on 23 June 2024).
- EU Agency For Fundamental Rights (2020), "Coronavirus COVID-19 outbreak in the EU Fundamental Rights Implications (Spain)" available at: https://fra.europa.eu/sites/default/files/fra_uploads/spain-report-covid-19-april-2020_en.pdf (accessed on 23 June 2024).
- EU Agency for Fundamental Rights Report (2020) "Coronavirus pandemic in the EU-Fundamental Rights Implications" available at: https://fra.europa.eu/sites/default/files/fra_uploads/es_report_on_coronavirus_pandemic_may_2020.pdf, (accessed on 23 June 2024).
- EU Commission (2020) Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID19 crisis, in particular concerning mobile applications and the use of anonymised mobility data
- EU Commission, Interoperability https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043 (accessed on 23 June 2024).
- European Centre for Disease Prevention and Control (2020) "Mobile applications in support of contact tracing for COVID-19 – A guidance for EU/EEA Member States", Stockholm: ECDC, available at: <https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing> (accessed on 23 June 2024).
- European Centre for Disease Prevention and Control (ECDC), (2020) "The guidance provided by the European Centre for Disease Prevention and Control," <https://www.ecdc.europa.eu/en/publications-data/guidance> (accessed on 23 June 2024).
- European Commission Website, European approach on data protection law see European Commission, Data Protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 23 June 2024).
- European Commission Website, Mobile Contact Tracing Apps https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (accessed on 23 June 2024).
- European Commission, (2022) Digital Contact Tracing Study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing to combat and exit the COVID-19 pandemic VIGIE 2021-0649 Framework Contract SMART 2019/0024, Lot 2 <https://commission.europa.eu/system/files/2023-02/DigitalContactTracingStudy.pdf> (accessed 23 June 2024).
- European Commission, Data Protection by Design and by Default https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (accessed on 23 June 2024).
- European Commission, interoperability gateway for tracing and warning apps available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1905#privacy (accessed on 23 June 2024).
- European Commission, Mobile Contact Tracing Apps https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (accessed on 15 August 2022).
- European Commission, National Joint Controllers and privacy policies, https://health.ec.europa.eu/document/download/f2460691-b730-4be5-87d4-474afe09a7fb_en (accessed on 2 June 2024).
- European Commission, Principles of GDPR https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en (accessed on 23 June 2024).

- European Parliament Briefing ITRE in Focus, National COVID-19 contact tracing apps available at [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI\(2020\)652711_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf) (accessed on 23 June 2024).
- European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html (accessed on 23 June 2024).
- Geneva Center of Humanitarian Studies (2022) “Emergencies and human rights in times of COVID-19”, available at: <https://humanitarianstudies.ch/emergencies-and-human-rights-in-times-of-covid-19/> (accessed on 23 June 2024).
- Gobierno De España, Ministerio Del Interior, (2023) “Right of Access to the File “PERPOL” https://sede.policia.gob.es/portalCiudadano/en/tramites_ciudadania_antecedentespoliciales_derechoacceso.php# (accessed on 23 June 2024).
- ICO, (2023) Contracts available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/contracts/> (accessed on 15 February 2024).
- ICO, (2023) Data Protection by Design and Default <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dgd2> (accessed on 23 June 2024).
- ICO, (2023) Data Protection Impact Assessment article available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#:~:text=A%20Data%20Protection%20Impact%20Assessment,some%20specified%20types%20of%20processing.> (accessed on 23 June 2024).
- ICO, (2023) Guide on Principle (a): Lawfulness, fairness and transparency <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> (accessed on 23 June 2024).
- ICO, (2023) Integrity and Confidentiality <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/> (accessed on 23 June 2024).
- ICO, (2023) Lawful Basis for Processing <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (accessed on 23 June 2024).
- ICO, (2023) Lawful basis for processing, available at: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing-1-0.pdf> (accessed on 23 June 2024).
- ICO, (2023) Purpose Limitation https://ico-org-uk.translate.google.com/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/?x_tr_sl=en&x_tr_tl=tr&x_tr_hl=tr&x_tr_pto=op,sc#limitation_principle (accessed on 23 June 2024).
- ICO, COVID-19 Contact tracing: data protection expectations on app development available at: <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf> (accessed on 23 June 2024).
- Information from the processor to the joint controllers regarding the European Federation Gateway Service for the purpose of their Data Protection Impact Assessments (DPIA-Draft).
- Informe de Evaluación de Impacto relativa a la Protección de Datos Tratamiento Radar Covid” available at: <https://rightsinternationalspain.org/wp-content/uploads/2022/03/Informe-de-Evaluacio%CC%81n-de-Impacto-relativa-a-la-Proteccio%CC%81n-de-Datos-Tratamiento-Radar-COVID.pdf> (accessed 23 June 2024).

- Instituto Nacional de Estadística Website <https://www.ine.es/> (accessed 23 June 2024).
- International Press Institute Website: <https://ipi.media/guest-article-covid-19-contact-tracing-apps-a-threat-to-press-freedom-and-journalists-privacy/> (accessed 23 June 2024).
- Ministerio de Sanidad (2020), "Procedimiento De Actuación Frente A Casos De Infección Por El Nuevo Coronavirus (Sars-Cov-2)" (14 March 2020). http://www.aeemt.com/web/wp-content/uploads/2020/03/2020-03-14_-Procedimiento-COVID_19.docx.pdf (accessed 23 June 2024).
- Ministerio de Transformación Digital Website <https://sedediadid.mineco.gob.es/en-us/procedimientos/electronicos/Paginas/detalle-procedimientos.aspx?IdProcedimiento=2> (accessed 23 June 2024).
- Ministerio de Transportes y Movilidad Sostenible, "Studio de movilidad con Big Data durante la pandemia" <https://www.mitma.gob.es/ministerio/covid-19/evolucion-movilidad-big-data> (accessed 19 June 2024).
- Office of Privacy Commissioner for Personal Data, Hong Kong (PCPD), "Data privacy issues relating to COVID-19 contact tracing apps" https://www.pcpd.org.hk/english/news_events/newspaper/newspaper_20210329.html (accessed 23 June 2024).
- Rights International Spain Report, (2021) "Tracking Apps in the EU Lessons for Future Use of Technology in Combating Social Challenges the Spanish Case: Radar Covid Application", (accessed 23 June 2024).
- The European Commission Website, "Principles of the GDPR, Purpose of Data Processing" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing_en (accessed 23 June 2024).
- The European Commission, (2020) "Analysing mobile apps that emerged to fight the COVID-19 crisis" https://joint-research-centre.ec.europa.eu/system/files/2023-01/03.covid-19_technical_report_final.pdf (accessed 23 June 2024).
- The Law Library of Congress, Global Legal Research Directorate (2020) "Regulating Electronic Means to Fight the Spread of COVID-19" <https://tile.loc.gov/storage-services/service/ll/lglrd/2020714995/2020714995.pdf> (accessed 23 June 2024).
- United Nations (2020) "Emergency Measures and Covid-19", https://www.ohchr.org/sites/default/files/Documents/Events/EmergencyMeasures_COVID19.pdf (accessed 23 June 2024).
- World Health Organization, (2020) "Ethical consideration to guide the use of digital proximity tracing technologies for COVID-19 contact tracing interim guidance 28 May 2020", https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics>Contact_tracing_apps-2020.1 (accessed 23 June 2024).
- World Health Organization, (2021) "Contact tracing in the context of COVID-19, interim guidance", available at: https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y (accessed 23 June 2024).
- World Health Organization, (2022) "Surveillance, case investigation and contact tracing for monkeypox: interim guidance, 25 August 2022", WHO Reference Number: WHO/MPX/Surveillance/2022.3, <https://www.who.int/publications/i/item/WHO-MPX-Surveillance-2024.1> (accessed 23 June 2024).

Jurisprudence:

- AEPD, (2021) Resolución De Procedimiento Sancionador Expediente N.º: PS/00222/2021.
- AEPD, (2021) Resolución De Procedimiento Sancionador Expediente N.º: PS/00233/2021.
- AEPD, (2022) Recurso de reposición N.º RR/00189/2022 .

- AEPD, Procedimiento N°: PS/00240/2019 available at: <https://www.aepd.es/documento/ps-00240-2019.pdf> (accessed on 15 June 2024).
- Datatilsynet (Norwegian Data Protection Authority), Temporary suspension of the Norwegian Covid-19 contact tracing app <https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/> (accessed on 20 June 2024).
- Datatilsynet Stament (Norwegian Data Protection Authority), Østre Toten Kommune <https://www.datatilsynet.no/contentassets/4609027cf9504e9aa12c3f05b45bdcf7/varsel-om-vedtak-om-overtredelsesgebyr-og-palegg.pdf> (accessed on 23 June 2024).
- Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, https://edpb.europa.eu/sites/default/files/files/file1/edpb_bindingdecision01_2020_en.pdf
- Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022] (OJ L 183 19.07.2018, p. 23, ELI: <http://data.europa.eu/eli/dec/2018/1022/oj>).
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (German Data Protection Authority), Datenschutz bei Corona-Warn-App ausreichend (in German) https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/12_Corona-Warn-App.html (accessed on 23 June 2024).
- Dissenting opinion of Judge Maria Luisa Balaguer Calalejon, member of Constitutional Court, see “Fundamento Jurídico 5” of Sentencia del Tribunal Constitucional 148/2021, de 14 de Julio (Boe Núm. 182, de 31 de julio de 2021), pp. 28-33.
- EDPB, Dutch DPA fines municipality for Wi-Fi tracking https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en#:~:text=The%20Dutch%20Data%20Protection%20Authority,work%20in%20the%20city%20centre. (accessed on 23 June 2024).
- EDPB, Danish Data Protection Agency Proposes 12 Million DKK Fine https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en (accessed on 12 August 2022).
- EDPB, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, available at : https://edpb.europa.eu/sites/default/files/files/file1/edpb_bindingdecision01_2020_en.pdf,
- EDPB, Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) available at: https://edpb.europa.eu/sites/default/files/decisions/nl_2020-09-02_-_dpia_list_nl_sa_-_national_decision_en.pdf
- EDPB, Temporary suspension of the Norwegian Covid-19 contact tracing app https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en (accessed on 23 August 2022).
- European Commission For Democracy Through Law (Venice Commission), Judgment of The Constitutional Court of Spain of 19 November 2020.
- European Court of Human Rights, Ben Faiza v. France, 2018, available at: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-180657%22%7D> (accessed on 23 June 2024).
- European Court of Human Rights, Guide to the Case-Law of the of the European Court of Human Rights, Data protection, Updated on 30 April 2022, available at: https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, (accessed on 23 June 2024).
- European Court of Human Rights, Uzun v. Germany, 2010 (Application no. 35623/05) case available at: <https://hudoc.echr.coe.int/eng#%7B%22languageisocode%22:%5B%22ENG%22%5D,%22appno%22%5B%2235623%22%5D%7D>

[2:\[%2235623/05%22\],%22documentcollectionid%22:\[%22CHAMBER%22\],%22itemid%22:\[%22001-100293%22\] \(accessed on 23 June 2024\).](#)

- Formal Comments of the EDPS on the Proposal for a Regulation amending Council Regulation (EC) No 1224/2009, and amending Council Regulations (EC) No 768/2005, (EC) No 1967/2006, (EC) No 1005/2008, and Regulation (EU) No 2016/1139 of the European Parliament and of the Council as regards fisheries controls available at https://edps.europa.eu/sites/default/files/publication/18-07-18_edps_formal-comments_dg_mare_en.pdf (accessed on 23 June 2024).
- Garante (Italian Data Protection Authority), App "Immuni": via libera del Garante privacy <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9356588> (accessed on 23 June 2024).
- Gegevensbeschermingsautoriteit (Belgium Data Protection Authority), Beslissing ten gronde 48/2022 van 4 april 2022 Deze beslissing werd gedeeltelijk vernietigd ten aanzien van de eerste verweerder en geheel vernietigd ten aanzien van de tweede verweerder door het arrest 2022/AR/560&564 van het Marktenhof dd. 7 december 2022, (in Dutch) <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-48-2022.pdf> (accessed on 23 June 2024).
- Informacijski pooblaščenec (Slovenian Data Protection Authority), Opinions prior to the application of the General Regulation (before 25.5.2018), Mnenja pred začetkom uporabe Splošne uredbe (pred 25.5.2018) https://www.ip-rs.si/vop?tx_jzgdprdecisions_pi1%5BshowUid%5D=1504 (accessed on 23 June 2023).
- Judgment of The Court (First Chamber) 12 Jan 2023, RW v. Österreichische Post AG, REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings <https://curia.europa.eu/juris/document/document.jsf?jsessionid=3C5CC72DC7FD40E09826387758207064?text=&docid=269146&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=175897> (accessed on 5 April 2023).
- Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Request for a preliminary ruling from the Audiencia Nacional. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> (accessed on 5 April 2023).
- Liberties, Decisions and Recommendations of Data Protection Authorities in Europe <https://www.liberties.eu/en/stories/trackerhub2-dpa-decisions/43529> (accessed on 23 June 2024).
- Prezes Urzędu Ochrony Danych Osobowych (UODO) (Polish Data Protection Authority) Summary of the “record fine imposed on controller for personal data breach’ decision <https://uodo.gov.pl/en/553/1311> (accessed on 24 June 2024).
- Prezes Urzędu Ochrony Danych Osobowych, (UODO) (Polish Data Protection Authority) Decision DKN.5130.2215.2020 <https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020> (available in Polish) (accessed on 24 June 2024).
- Prezes Urzędu Ochrony Danych Osobowych, (UODO) (Polish Data Protection Authority) DOL.023.462.2020.WL.OJ (in Polish) <https://bip.brpo.gov.pl/sites/default/files/Odpowied%C5%BA%20PUODO,%2019.06.2020.pdf> (accessed on 20 June 2024).
- Question for written answer E-005833/2020 to the Commission, Rule 138 Lídia Pereira (PPE), Paulo Rangel (PPE), José Manuel Fernandes (PPE), Álvaro Amaro (PPE), Maria da Graça Carvalho (PPE), Cláudia Monteiro de Aguiar (PPE) Subject: Mandatory installation of contact tracing apps and personal data protection during pandemic https://www.europarl.europa.eu/doceo/document/E-9-2020-005833_EN.html (accessed 11 November 2022).

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 Annex 2: Examples Of Supplementary Measures, 28.
- Recurso de reposición N° RR/00189/2022, Examinado el recurso de reposición interpuesto por SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL (en lo sucesivo, la SEDIA) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00222/2021
- State Data Protection Inspectorate (Lithuanian Data Protection Authority) (DPA) “The Fine Issued for Infringements of the GDPR in Mobile Application “Karantinas” <https://vdai.lrv.lt/uploads/vdai/documents/files/2021%20App%20Karantinas.pdf> (accessed on 23 June 2024).
- Tribunal Constitucional de España, Sentencia 148/2021, de 14 de julio (Boe Núm. 182, de 31 de Julio De 2021), ECLI:Es:Tc:2021:148.
- Tribunal Supremo. Sala de lo ATS 3375/2021 - ECLI:ES:TS:2021:3375A Contencioso <https://www.poderjudicial.es/search/documento/AN/9470383/actos%20y%20procedimien%20administrativo/20210330> (accessed on 23 June 2024).

Relevant Regulations

- Consolidated Version of Treaty on European Union https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (accessed on 15 August 2022).
- Constitución Española, Passed by the Cortes Generales in Plenary Meetings of the Congress of Deputies and the Senate held on October 31, 1978 Ratified by the Spanish people in the referendum of December 6, 1978 Sanctioned by His Majesty the King before the Cortes on December 27, 1978.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- EEA Agreement, Annex XI, Protocol 37, amended by Decision of the EEA Joint Committee No 154/2018, of 6 July 2018.
- European Convention On Human Rights <https://www.echr.coe.int/european-convention-on-human-rights> .
- International Covenant on Civil and Political Rights (ICCPR), entry into force: 23 March 1976, in accordance with Article 49 available at: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. «BOE» núm. 295, de 10/12/2013.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. «BOE» núm. 295, de 10/12/2013.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. <https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392>.
- Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio. «BOE» núm. 134, de 05/06/1981. <https://www.boe.es/buscar/act.php?id=BOE-A-1981-12774>.
- Order SND/297/2020, of March 27, entrusting the Secretary of State for Digitization and Artificial Intelligence, of the Ministry of Economic Affairs and Digital Transformation, with

the development of various actions to manage the health crisis caused by COVID-19”, available at: <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-4162>.

- Order SND/404/2020 (Minister of Health) (11 May 2020). <https://www.boe.es/buscar/act.php?id=BOE-A-2020-4933>.
- Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. «BOE» núm. 67, de 14/03/2020. <https://www.boe.es/buscar/act.php?id=BOE-A-2020-3692>.
- Real Decreto 555/2020, de 5 de junio, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. <https://www.boe.es/buscar/act.php?id=BOE-A-2020-5767#a1>.
- Real Decreto de 24 de julio de 1889, mandando insertar en la «gaceta» el texto de la nueva edición del código civil con las enmiendas y adiciones propuestas por la sección de lo civil de la comisión de codificación.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
- Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID"(«BOE» núm. 273, 15 de octubre de 2020, BOE-A-2020-12339).
- Resolución de 30 de abril de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y Telefónica Digital España, SLU, para la operación de la Aplicación ASISTENCIACOVVID19 en el contexto de la situación de crisis sanitaria ocasionada por el COVID-19. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4829 (BOE» núm. 125, de 5 de mayo de 2020. BOE-A-2020-4829).
- Resolución de 8 de mayo de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Comunidad Autónoma de Castilla-La Mancha, sobre la adhesión al uso de la Aplicación AsistenciaCOVID19 («BOE» núm. 150, de 27 de mayo de 2020, páginas 35080 a 35099 (20 págs.).
- Royal Decree-law 21/2020 (9 June 2020), <https://www.boe.es/buscar/act.php?id=BOE-A-2020-5895>.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Aug 20, 1996.

Privacy Policies, Terms of Use, Technical Specifications and Other Relevant Documentations of Contact Tracing Applications:

- Apturi Covid, Privacy Policy <https://apturicovid.lv/privatuma-politika/#en> (accessed on 23 June 2024).
- Apturi Covid, Git Hub <https://github.com/ApturiCOVID/apturicovid-android> (accessed on 23 June 2024).
- Apturi Covid, Terms of Use <https://www.spkc.gov.lv/lv/media/15181/download> (accessed on 23 June 2024).
- Asistencia Covid, Privacy Policy <https://asistencia.covid19.gob.es/politica-de-privacidad> (accessed on 3 January 2023).
- Asistencia COVID19, Terms of Use, <https://asistencia.covid19.gob.es/condiciones-de-uso> (accessed on 3 January 2023).
- Corona Alert, Privacy Statement <https://coronalert.be/en/privacy-statement/> (accessed on 23 January 2024).

- Corona Alert, DPIA https://coronalert.be/wp-content/uploads/2021/07/DPIA_contactopsporingsapplicatie_BelgieV.8_NL_versie_17062021.pdf (accessed on 23 June 2024).
- Corona Madrid, Privacy Policy- (Updated) <https://coronavirus.comunidad.madrid/politica-de-privacidad/> (accessed on 27 January 2024).
- Corona Madrid, Privacy Policy <https://www.coronamadrid.com/proteccion-de-datos> (accessed on 22 January 2023).
- Corona Melder, DPIA <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlbqlspueffm> (accessed on 6 June 2024).
- Corona Melder, Git Hub Source Code <https://github.com/minvws> (accessed on 23 June 2024).
- Corona Melder, Privacy Policy <https://coronamelder.nl/en/privacy> (accessed on 3 April 2023).
- Corona Warn, DPIA https://www.fiff.de/dsfa-corona-file-en/at_download/FlfF-CoronaApp-DSFA-EN-v1.6.pdf (accessed on 23 June 2024).
- Corona Warn, GitHub, <https://github.com/corona-warn-app> (accessed on 23 June 2024).
- Corona Warn, Notice of Termination <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).
- Corona Warn, Overview Security, Secure development <https://github.com/corona-warn-app/cwa-documentation/blob/main/overview-security.md> (accessed on 23 June 2024).
- Corona Warn, Privacy <https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf> (accessed on 22 January 2024).
- Corona Warn, Solution Architect https://github.com/corona-warn-app/cwa-documentation/blob/main/solution_architecture.md#mobile-applications (accessed on 8 June 2024).
- Corona Warn, Terms of Use Statement <https://www.coronawarn.app/assets/documents/cwa-eula-en.pdf> (accessed on 22 July 2023).
- Coronalert App, Git Hub <https://github.com/covid-be-app/cwa-app-android> (accessed on 23 June 2024).
- Covid Alert (Malta) Git Hub Source Code <https://github.com/GOVMT-MITA> (accessed on 23 June 2024).
- COVID Alert Malta, Privacy policy <https://covidovidalert.gov.mt/privacy-policy/> (accessed on 19 April 2023).
- COVID Tracker App, Git Hub, <https://github.com/HSEIreland/covid-tracker-app> (accessed on 23 June 2024).
- COVID-19.eus/Collaboro, Privacy Policy <https://colaboro.erictel.com/privacy/> (accessed on 27 June 2024).
- COVIDAlert App, Git Hub, <https://github.com/GOVMT-MITA> (accessed on 23 June 2024).
- CovTracer-EN Git Hub Source Code <https://github.com/CovTracer-EN/covtracer-en-app> (accessed on 23 June 2024).
- CovTracer-EN, Privacy policy https://covtracer.dmrid.gov.cy/dmrid/covtracer/covtracer.nsf/covtracer02_en/covtracer02_en?opendocument (accessed on 23 June 2024).
- E-Estonia Website, HOIA the product of a unique private and public partnership <https://e-estonia.com/estonias-coronavirus-app-hoia-the-product-of-a-unique-private-public-partnership/> (accessed on 23 June 2024).
- eRouska, Audit Report <https://erouska.cz/en/audit-kod> (accessed on 9 June 2024)
- eRouska Application Terms and Conditions, Information on Personal Data Processing of eRouska 2.0. Application, <https://erouska.cz/en/podminky-pouzivani#osobni> (accessed on 23 June 2024), <https://erouska.cz/en/podminky-pouzivani#osobni> (accessed on 23 June 2024).

- European mHealth Hub, Radar Covid <https://mhealth-hub.org/radar-covid> (accessed on 23 June 2024).
- Gateway, National Joint Controllers and privacy policies, available at: https://health.ec.europa.eu/system/files/2023-02/gateway_jointcontrollers_en.pdf (accessed on 23 June 2024).
- Gateway Initiative https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904 (accessed on 23 June 2024).
- HOIA, Closure Statement <https://www.tehik.ee/uudis/maikuust-suletakse-hoia-rakendus> (accessed on 23 June 2024).
- HOIA, Git Hub <https://koodivaramu.eesti.ee/tehik/hoia/documentation> (accessed on 23 June 2023).
- HOIA, Privacy Policy <https://koodivaramu.eesti.ee/tehik/hoia/app-web/-/blob/master/content/privacy.en.md> (accessed on 23 June 2024).
- HSE, data protection policy, <https://www.hse.ie/eng/gdpr/hse-data-protection-policy/> (accessed on 8 June 2024).
- HSE, DPIA <https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%202026.06.2020.pdf> (accessed on 23 June 2024).
- HSE, Irish Contact Tracing Application, EDPB Compliance Assessment, <https://github.com/HSEIreland/> (accessed on 23 June 2024).
- HSE, Irish Contact Tracing Application, EU Toolbox Compliance Assessment, <https://github.com/HSEIreland/> (accessed on 23 June 2024).
- HSE, Privacy <https://www2.hse.ie/services/covid-tracker-app/data-protection-information-notice.html> (accessed on 23 June 2024).
- <https://sem.gencat.cat/ca/061-salut-respon/apps-mobils/STOPCOVID19/condicions-seguretat/> (accessed on 27 June 2024).
- Immuni, Git Hub Source Code <https://github.com/immuni-app/immuni-documentation> (accessed on 23 June 2024).
- Immuni, Privacy Documentation <https://github.com/immuni-app/immuni-documentation#privacy> (accessed on 23 June 2024).
- Immuni, Security <https://github.com/immuni-app/immuni-documentation/tree/master> (accessed on 23 June 2024).
- Korona Stop, Privacy Policy <https://koronastop.lrv.lt/uploads/documents/files/corona-stop-app/Privatumo-politika-korona-stop-en.pdf> (accessed on 23 June 2024).
- Korona Vilkku, Compliance Statement <https://tietoturvamerkki.fi/sites/default/files/media/file/statement-of-compliance-thl-koronavilkku.pdf> (accessed on 23 June 2024).
- Korona Vilkku, Privacy policy <https://koronavilkku.fi/en/privacy/> (accessed on 22 January 2023).
- Ostani Zdrav, Functioning of the application, <https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanizdrav-mobile-application/functioning-of-the-application/> (accessed on 23 June 2024).
- OstaniZdrav, General Information Document, Mobilná Aplikácia Covid19 Zostaň Zdravý - Koronavírus A Slovensko (Gov.Sk), <https://korona.gov.sk/mobilna-aplikacia-covid19-zostan-zdravy/> (accessed on 23 June 2024).
- OstaniZdrav, Git Hub, <https://github.com/si-covid-19> (accessed on 23 June 2024).
- OstaniZdrav, Privacy Notice available at: <https://www.gov.si/assets/vlada/Koronavirus-zbirno-infografike-vlada/APP-OstaniZdrav/Privacy-notice.pdf> (accessed on 23 June 2024).
- Protego Safe Application, Terms of Use, <https://www.gov.pl/web/protegosafe/dokumenty> (accessed on 23 June 2024).
- ProtegoSafe DPIA <https://www.gov.pl/web/protegosafe/dokumenty> (accessed on 23 June 2024).

- ProteGOSafe Git Hub Source Code <https://github.com/ProteGO-Safe> (accessed on 23 June 2024).
- Radar Covid- Análisis de Riesgos Sistema de Información Radar Covid-19” available at: <https://rightsinternationalspain.org/wp-content/uploads/2022/03/Ana%CC%81lisis-de-riesgos-agosto-2020.pdf> (accessed 23 June 2024).
- Radar Covid, FAQs Utilizando las últimas tecnologías para contener la pandemia COVID-19 <https://radarcovid.gob.es/> (accessed on 23 June 2024).
- Radar Covid, Git Hub, <https://github.com/radarcovid> (accessed on 23 June 2024).
- Radar Covid, Manifest <https://radarcovid.gob.es/manifiesto> (accessed on 23 June 2024).
- Radar Covid, Privacy Policy, <https://radarcovid.gob.es/en/privacy-policy> (accessed on 23 June 2024).
- Radar Covid, Technical Issues, Git Hub, available at: <https://github.com/RadarCOVID/radar-covid-android/issues/47> (accessed on 23 June 2024).
- Radar Covid, Terms and Conditions <https://radarcovid.gob.es/condiciones-de-uso> (accessed on 23 June 2024).
- Rakning C-19, Covid-19 Tracing App Privacy policy www.covid.is/app/privacystatement (accessed on 10 January 2023).
- Rakning C-19, Git Hub Source Code <https://github.com/aranja/rakning-c19-app> (accessed on 23 June 2024).
- Smittestopp (Denmark), DPIA https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (accessed on 6 June 2024).
- Smittestopp App, Git Hub, <https://github.com/Sundhedsdatastyrelsen> (accessed on 23 June 2024).
- Smittestopp (Denmark), Processing of Personal Data <https://smittestopp.dk/en/data-protection/> (accessed on 11 January 2024).
- Smittestopp (Norway), Privacy Policy <https://www.fhi.no/en/about/smittestop/use-of-smittestopp-privacy-policy> (accessed on 11 August 2023).
- Smittestopp Git Hub Source Code <https://github.com/folkehelseinstituttet/Fhi.Smittestopp.App> (accessed on 23 June 2024)
- Stayaway, General Statement <https://github.com/stayawayinesctec> (accessed on 22 July 2023).
- StayAway, Git Hub Source Code <https://github.com/stayawayinesctec/stayaway-app> (accessed on 23 June 2024).
- Stayaway, Privacy policy <https://stayawaycovidovid.pt/privacy-policy/> (accessed on 10 February 2022).
- Stop Corona App, Git Hub <https://github.com/austrianredcross> (accessed on 23 June 2024).
- Stop Covid, Privacy Policy <https://stopcovid19.zdravlje.hr/html/privacy-policy.html> (accessed on 23 June 2024).
- Stop COVID-19 App, Git Hub <https://github.com/covid-be-app/cwa-app-android> (accessed on 23 June 2024).
- Stop Covid-19, Condicions de seguretat de l'app STOPCOVID19.
- Stop Covid-19, Functional Document, https://stopcovid19.cat/wp-content/uploads/2020/07/Funcional-STOPCOVID19-CAT_CatSalut_EN.pdf (accessed on 27 June 2024).
- Stop-Covid-19, DPIA https://www.koronavirus.hr/uploads/Stop_COVID_19_Data_Protection_Impact_Assessment_Summary_2020_11_16_58dea76816.pdf (accessed on 23 June 2024).
- StopCovid-ProteGo Documents, Privacy Policy <https://www.gov.pl/web/protegosafe/dokumenty> ((accessed on 23 June 2024).

- SwissCovid, Git Hub Source Code <https://github.com/SwissCovid> (accessed on 23 June 2024).
- Tous Anti Covid, Activity Report, https://sante.gouv.fr/IMG/pdf/rapport_tousanticovid_mars_2023.pdf (accessed on 22 March 2024).
- Tous Anti-Covid, Privacy <https://bonjour.tousanticovid.gouv.fr/privacy-en.html> (accessed on 22 March 2024).
- Tous Anti-Covid, Technical Specifications, https://sante.gouv.fr/IMG/pdf/rapport_tousanticovid_mars_2023.pdf (accessed on 9 June 2024).
- Zostaň Zdravý, General Information Document, Mobilná Aplikácia Covid19 Zostaň Zdravý - Koronavírus A Slovensko (Gov.Sk), <https://korona.gov.sk/mobilna-aplikacia-covid19-zostan-zdravy/> (accessed on 2 June 2024).

Articles, Reports and Other Relevant Documentation Published on Websites:

- ABC, Amazon to provide cloud services for coronavirus tracing app <https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682> (accessed on 12 June 2024).
- Amazon, Covid-19 Contact Tracing Platform <https://aws.amazon.com/marketplace/pp/prodview-gsckcplivo452> (accessed on 7 January 2021).
- Amazon, Privacy Policy available at: <https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ> (accessed on 11 August 2022).
- AppCensus Report (2020) “COVID-19 Android Apps: Spain App Analysis Report”, <https://blog.appcensus.io/wp-content/uploads/2020/04/report.pdf> (accessed on 27 June 2024).
- Apple Website, Apple and Google Partner on Covid-19 Contact Tracing Technology <https://www.apple.com/pl/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> (accessed on 15 August 2022).
- Apple, Privacy Policy <https://www.apple.com/legal/privacy/en-ww/> (accessed on 11 August 2022).
- Apple, Privacy-Preserving Contact Tracing, see <https://www.apple.com/covid19/contacttracing/> (accessed on 16 October 2023).
- Arbuckle, Luk (2020) “Aggregated Data Provides a False Sense of Security”, IAPP <https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/> (accessed on 22 June 2024).
- BBVA, (2020) How Do Covid-10 Tracing Apps Work and What Kind of Data Do They Use? <https://www.bbva.com/en/how-do-covid-19-tracing-apps-work-and-what-kind-of-data-do-they-use/> (accessed on 15 August 2022).
- Binnia, Isla (2020) “Spain's COVID tracing app tries to balance public health with privacy” Reuters, <https://www.reuters.com/article/us-health-coronavirus-apps-spain-idUKKBN2680SF> (accessed on 23 June 2024).
- Carrasco, Sergio (2021) “The Failure of Spain’s Radar Covid App” , Liberties available at: <https://www.liberties.eu/en/stories/app-radar-covid-rights/43524> (accessed on 22 June 2024).
- Colin Barker, (2014) “ Big data must operate within data protection law,” says watchdog, “and here’s how”, ZDNET <https://www.zdnet.com/article/big-data-must-operate-within-data-protection-law-says-watchdog-and-heres-how/> (accessed on 19 November 2023).
- Colome Perez, Jordi (2020) “La ‘app’ Radar Covid ha tenido una brecha de seguridad desde su lanzamiento “, El Pais <https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html> (accessed on 22 June 2024).

- Díaz, Efrén (2021) "Geolocation Apps Do not Cure Covid-19 They Analyze Peoples Mobility", Geospatial World, available at: <https://www.geospatialworld.net/article/geolocation-apps-do-not-cure-covid-19-they-analyze-peoples-mobility/> (accessed on 23 June 2024).
- Dilmegani, Cem (2024) "Differential Privacy: How It Works, Benefits & Use Cases in 2024". AI Multiple Research, <https://research.aimultiple.com/differential-privacy/> (accessed on 23 June 2024).
- DPO centre, (2020) Due diligence what you need to consider <https://www.dpocentre.com/vendor-due-diligence-what-you-need-to-consider/> (accessed on 20 June 2024).
- Dravalou, Elisavet (2021) "What "technical and organisational measures" actually means" DP Organizer, available at: <https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/> (accessed on 22 June 2024).
- Duarte, Diogo (2019) "Art. 37 GDPR: Which are the "Core Activities" of the entities?" available at: <https://www.linkedin.com/pulse/art-37-gdpr-which-core-activities-entities-diogo-duarte> (accessed on 5 March 2024).
- Duball, Joe (2020), "Centralized vs Decentralized Contact Tracing", IAPP, <https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/> (accessed on 12 June 2024).
- Duke TechPolicy Sanford Article (2021) "Comparing centralized and decentralized contact-tracing approaches" available at: <https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/> (accessed on 17 March 2024).
- DW Website, German police under fire for misuse of COVID app <https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597> (accessed on 22 June 2024).
- Esguera, Richard (2011) "An Introduction to the Federated Social Network," EFF, <https://www.eff.org/deeplinks/2011/03/introduction-distributed-social-network> (accessed on 22 June 2024).
- Facebook, Privacy Policy <https://www.facebook.com/about/privacy/previous> (accessed on 11 August 2022).
- Google, Privacy Policy <https://policies.google.com/privacy?hl=en-US> (accessed on 11 August 2022).
- Hoeksma, Jon (2020) "Norway forced to backtrack on mass surveillance track and trace app." Digital Health, available at: <https://www.digitalhealth.net/2020/06/norway-track-and-trace-app/> (accessed on 15 June 2024).
- Hoffman-Andrews, Jacob, and Crocker, Andrew (2020) "How to protect Privacy When Aggregating Location Data Fight Covid-19", Electronic Frontier Foundation <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed on 22 June 2024).
- Hunton, Andrews Kurth, (2020) "Article 29 WP clarified purpose limitation principle on big and open data", Hunton Privacy Blog available at: <https://www.huntonprivacyblog.com/2013/04/09/article-29-working-party-clarifies-purpose-limitation-principle-opines-on-big-and-open-data/> (accessed on 22 June 2024).
- IAPP, Layered Notice <https://iapp.org/resources/article/layered-notice/> (accessed on 23 June 2024).
- Jeirussen, Simone (2021) "Why Less is More When it Comes to Data?", Towards Data Science, <https://towardsdatascience.com/why-less-is-more-when-it-comes-to-data-8b90619fdeaf> (accessed on 23 June 2024).
- Kyotu Technology Report (2020) "Unveiling the impact of covid tracking apps around the globe" <https://www.kyotutechnology.com/unveiling-the-impact-of-covid-tracking-apps-around-the-globe/> (accessed on 23 June 2024).

- Lomas, Natasha (2020), "EU lawmakers set out guidance for coronavirus contacts tracing apps" Tech Crunch available at: <https://techcrunch.com/2020/04/16/eu-lawmakers-set-out-guidance-for-coronavirus-contacts-tracing-apps/> (accessed on 15 June 2024).
- Maldita Website, Asistencia Covid-19, la app de autodiagnóstico del gobierno, sólo te geolocaliza si la descargas y activas esta opción al empezar el test <https://maldita.es/malditatecnologia/20200406/asistencia-covid-19-app-autodiagnostico-gobiernosolo-geolocaliza-localizacion-descarga/> (accessed 23 June 2024).
- Margherita Russo, Claudia Cardinale Ciccotti, Fabrizio De Alexandris, Antonela Gjinaj, Giovanni Romaniello, Antonio Scatorchia, Giorgio Terranova, CEPR VOXEU Website Article 02 August 2021 available at: <https://voxeu.org/article/cross-country-comparison-contact-tracing-apps>.
- Matheson, Lee (2018) "Top 10 Operational Responses to the GDPR – Part 6: Transparency and privacy notices", IAPP, [https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-6-transparency-and-privacy-notice/#:~:text=Pursuant%20to%20Article%2012\(1,the%20disclosure%20should%20be%20easily](https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-6-transparency-and-privacy-notice/#:~:text=Pursuant%20to%20Article%2012(1,the%20disclosure%20should%20be%20easily) (accessed on 15 June 2024).
- Mauro, Aaron (2020) "Coronavirus contact tracing poses serious threats to our privacy." The Conversation available at: <https://theconversation.com/coronavirus-contact-tracing-poses-serious-threats-to-our-privacy-137073> (accessed on 23 June 2024).
- Méndez-Monasterio Silvela, Pablo (2021) "Sobre la inconstitucionalidad del Real Decreto 463/2020 por el que se declara el Estado de alarma", Conflegal, <https://conflegal.com/20210723-opinion-sobre-la-inconstitucionalidad-del-real-decreto-463-2020-por-el-que-se-declara-el-estado-de-alarma/> (accessed on 22 June 2024).
- Merino, Marcos (2022) "La app Radar COVID violó 8 artículos de la normativa de protección de datos: la AEPD acaba de sancionar al Gobierno", Genbeta Website, available at: <https://www.genbeta.com/actualidad/app-radar-covid-violo-8-articulos-normativa-proteccion-datos-aepd-acaba-sancionar-al-gobierno> (accessed on 25 December 2023).
- Microsoft, Privacy Covid-19 Data Collection <https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/> (accessed on 15 August 2022).
- PricewaterhouseCoopers (PWC) (2020) "In the era of data protection, less data is more" <https://www.pwc.ch/en/publications/2020/In%20the%20era%20of%20data%20Protection.pdf> (accessed on 23 June 2024).
- Privacy International Website, Thailand: SIM card and app to track travellers <https://privacyinternational.org/examples/3452/thailand-sim-card-and-app-track-travellers> (accessed on 10 January 2021).
- Protecto Website Article, Common Problems in Handling Data Subject Access Requests <https://www.protecto.ai/blog/common-problems-in-handling-data-subject-access-requests-dsars> (accessed on 12 June 2024)..
- Reardon, Joel (2021) "Why Google Should Stop Logging Contact-Tracing Data?", AppCensus, <https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/> (accessed on 23 June 2024).
- Reus, Jurre and Bilderbeek, Nicole (2022) "Data Portability in the EU an Obscure: Data Subject Right", IAPP <https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/> (accessed on 23 June 2024).
- Reuters (2020), Poland rolls-out privacy secure coronavirus tracking app <https://www.reuters.com/article/us-health-coronavirus-poland-tech-idUSKBN23G208> (accessed on 23 June 2024).
- Rich, Jessica (2021), "How our outdated privacy laws doomed contact-tracing apps", Brookings Institute <https://www.brookings.edu/articles/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/> (accessed on 23 June 2024).
- Romero, Mario (2020) "Covid Radar, is it Safe?", H&A Group Publications available at: <https://www.hyaip.com/en/news/covid-radar-is-it-safe/> (accessed on 23 June 2024).

- García Mahamut, Rosario (2020) "Covid-19 and Data Protection in Spain: an overview" Blog Droit Europeen available at: <https://blogdroiteuropeen.com/2020/06/29/covid-19-and-data-protection-in-spain-an-overview-by-rosario-garcia-mahamut/> (accessed on 23 June 2024).
- Silvieira, Alessandra, Covelo de Abreu, Joana, Cabral, Tiago Sergio (2020) "The Mandatory Contact Tracing App: StayAway Covid: a Matter of European Union Law", Unio EU Law Journal <https://officialblogofunio.com/2020/10/20/the-mandatory-contact-tracing-app-stayaway-covid-a-matter-of-european-union-law/> (accessed on 23 June 2024).
- Soltani, Ashkan, Calo, Ryan and Bergstrom, Carl (2020) "Contact-tracing apps are not a solution to the COVID-19 crisis." Brookings Institution. United States of America, Why Contact Tracing Could be a Disaster? <https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/> (accessed on 10 June 2024).
- Statista, Número de casos confirmados de coronavirus en España a fecha de 30 de junio de 2023, por comunidad autónoma <https://es.statista.com/estadisticas/1100641/regiones-afectadas-por-el-covid-19-segun-los-casos-confirmados-espana/> (accessed on 6 October 2023).
- Tapia, Antonia and del Campo, Amelia (2018) "Legal Systems in Spain" Thompson Reuters, [https://uk.practicallaw.thomsonreuters.com/7-634-0207?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/7-634-0207?transitionType=Default&contextData=(sc.Default)&firstPage=true) (accessed on 27 June 2024).
- The Wall Street Journal (2020) "South Korea tracks virus patients travels and publishes them online" https://www.wsj.com/articles/south-korea-tracks-virus-patients-travelsand-publishes-them-online11581858000?mod=searchresults&page=1&pos=2&mod=article_online (accessed on 17 July 2023).
- Tirant (2021) "El TC estima parcialmente el recurso contra preceptos del Real Decreto 463/2020, que declaró el estado de alarma para la gestión del Covid-19" <https://tirant.com/actualidad-juridica/noticia-sentencia-estado-de-alarma/> (accessed on 22 June 2024).
- True Vault Website Article, What Are the Rights of Data Subjects Under GDPR <https://www.truevault.com/resources/compliance/what-are-the-rights-of-data-subjects-under-gdpr> (accessed on 12 April 2023).
- UDS Enterprise (2021) "Radar COVID app source code to be released next week" available at: <https://udsenterprise.com/en/radar-covid-app-source-code-released-next-week/> (accessed on 20 November 2023).
- Umawing, Jovi (2020) "Labs survey finds privacy concerns, distrust of social media rampant with all age groups", Malware Bytest, <https://www.malwarebytes.com/blog/news/2019/03/labs-survey-finds-privacy-concerns-trust-of-social-media-rampant-with-all-age-groups> (accessed on 24 June 2024).
- Unai, Mieza (2021) "How Health And Location Data Were Handled In Times Of Covid-19" Lozano Schindhelm SLP, <https://es.schindhelm.com/en/news-jusful/covid-19-unit/how-health-and-location-data-were-handled-in-times-of-covid19-e168040> (accessed on 23 August 2023).
- Utrilla, Dolores (2020), "Spanish Supreme Court clarifies legal framework of restrictive measures adopted under public health legislation" Lex-Atlas: Covid-19, available at: <https://lexatlas-c19.org/spanish-supreme-court-clarifies-legal-framework-of-restrictive-measures-adopted-under-public-health-legislation/> (accessed on 23 June 2024).
- Van Schendel, Olenka (2020) "Data masking: Anonymisation or pseudonymisation?", GRC World Forums, available at: <https://www.grcworldforums.com/data-management/data-masking-anonymisation-or-pseudonymisation/12.article> (accessed on 22 June 2024).
- Wes, Matt (2020) "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization", IAPP <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/> (accessed on 22 June 2024).

- Williams, John and Cohen, Bret (2020) “What does the CCPA's 'purpose limitation' mean for businesses?” IAPP, <https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses/#:~:text=Background,controllers%20may%20use%20personal%20informatio>[n](https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses/#:~:text=Background,controllers%20may%20use%20personal%20informatio) (accessed on 15 June 2024).
- Queen Mary University (2021) “Study Provides First Real-World Evidence of COVID-19 Contact Tracing App Effectiveness” available at: <https://medicalxpress.com/news/2021-01-real-world-evidence-covid-contact-app.html> (accessed on 22 December 2023)..
- Zegarra&Schipper Abogados Publication, (2022) “Consultores Agencia Española De Protección De Datos Confirma Sanción A Entidad Estatal Por Vulnerar Las Normas De Protección De Datos Mediante Aplicación Móvil (App) Contra La Covid-19” available at <https://www.zysabogados.pe/wp-content/uploads/2022/06/004.pdf> (accessed on 11 February 2024).
- Zumbun, Josh (2022) “When it comes to data sometimes less is more”, The Wall Street Journal <https://www.wsj.com/articles/when-it-comes-to-data-sometimes-less-is-more-11667554203> (accessed on 23 June 2024).