Privacy aspects of contact tracing applications in Europe and recommendations for their future use

Raif Baran Tombul
Universitat Autònoma de Barcelona
rbtombul@gmail.com
ORCID: 0000-0001-8175-9227

Received: 20/01/2023
Accepted: 08/05/2023
Published: 28/07/2023

Recommended citation: TOMBUL, R.B. (2023). "Privacy Aspects of Contact Tracing Applications in Europe and Recommendations for Their Future Use"**.** *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, *2*(2), 49-71. DOI: <https://doi.org/10.5565/rev/quadernsiee.54>

Abstract

The first global pandemic in the age of digitalism indicated that there might be new types of privacy risks stemming from the processing activities taking place within the scope of digital contact tracing activities. While the right to life of all individuals living in the community should be primarily protected, their right to privacy should also be considered. Therefore, a balance between privacy and public health should be struck by both regulators and data controllers. The purpose of this review is to analyze the compliance efforts of data controllers in Europe with the existing EU data protection regulations, and guidance, and draw lessons for the use of contact tracing applications within the scope of potential disaster scenarios that may arise in the future by reviewing the existing literature and the privacy policies of the applications.

Keywords: European Privacy Law; European Unión Law; Pandemic; Digital contact tracing; Data protection.

Resumen. *Aspectos de privacidad de las aplicaciones de rastreo de contactos en Europa y recomendaciones para su uso futuro*

La primera pandemia global en la era de la digitalización indicó que podría haber nuevos tipos de riesgos de privacidad, derivados de las actividades de procesamiento que tienen lugar dentro del alcance de las actividades de rastreo de contactos digitales. Si bien se debe proteger principalmente el derecho a la vida de todas las personas que viven en la comunidad, también se debe considerar su derecho a la privacidad. Por ello,

tanto los reguladores como los controladores de datos deben lograr un equilibrio entre la privacidad y la salud pública. El propósito de esta revisión es analizar los esfuerzos de cumplimiento de los controladores de datos en Europa con las regulaciones y guías de protección de datos existentes en la UE y extraer lecciones para el uso de aplicaciones de rastreo de contactos dentro del alcance de escenarios de desastres potenciales que puedan surgir en el futuro, mediante la revisión de la literatura existente y de las políticas de privacidad de las aplicaciones.

Palabras clave: Ley Europea de Privacidad; Derecho de la Unión Europea; Pandemia; Seguimiento de contactos digitales; Protección de datos.

Resum. *Aspectes de privadesa de les aplicacions de rastreig de contactes a Europa i recomanacions per al seu ús futur*

La primera pandèmia global a l'era de la digitalització va indicar que hi podria haver nous tipus de riscos de privadesa, derivats de les activitats de processament que tenen lloc dins l'abast de les activitats de rastreig de contactes digitals. Si bé cal protegir principalment el dret a la vida de totes les persones que viuen a la comunitat, també s'ha de considerar el seu dret a la privadesa. Per això, tant els reguladors com els controladors de dades han d'assolir un equilibri entre la privadesa i la salut pública. El propòsit d'aquesta revisió és analitzar els esforços de compliment dels controladors de dades a Europa, amb les regulacions i les guies de protecció de dades existents a la UE i extreure lliçons per a l'ús d'aplicacions de rastreig de contactes, dins l'abast d'escenaris de desastres potencials que puguin sorgir en el futur, mitjançant la revisió de la literatura existent i de les polítiques de privadesa de les aplicacions.

Paraules clau: Llei Europea de Privadesa; Dret de la Unió Europea; Pandèmia; Seguiment de contactes digitals; Protecció de dades.

Summary

1. INTRODUCTION

Contact tracing, in addition to robust testing, isolation, and care of cases, is an important strategy for tackling chains of transmission of SARS-CoV-2 and decreasing mortality associated with Covid-19.[1] Contact tracing methodologies have already been utilized for more than 500 years to control the great pox (also known as syphilis) once a group of Italian doctors started investigating the spread of the epidemic in the search for the "patient zero"(Scantamburlo et al., 2021). There are many samples in the history of medicine, ranging from AIDS to Ebola, where tracing methods were conducted to determine symptomatic people and, where required, employ isolation strategies (Scantamburlo et al., 2021). The objective of contact tracing activities is to break transmission chains by notifying others who have come into touch with an infected person that they are at a higher risk of infection and how to protect themselves from spreading the sickness to others. Therefore, it might be an efficient tool to tackle the spread of the pandemic in society. Accordingly, several European countries have used contact tracing applications to tackle the spread of the virus in society. However, at the same time, while implementing this activity, there are also other concerns associated with the privacy of the users in countries. In other words, tracking patients with Covid-19 and activities of contact persons could cause a breach of their privacy (Mbunge, 2020). Accordingly, it is of massive importance to determine each privacy and security-related risk to users and implement efficient safeguards. Although there is already a certain amount of discussion and research devoted to the privacy risks associated with contact tracing activities employed within Europe, this review is aiming to draw lessons for any potential use of contact tracing applications in the future so that data subjects will not hesitate the download these applications due to the privacy concerns. User trust is critical for adoption by enough users to render a contact tracing application effective (Blasimme et al, 2021). Missing guidance on the way contact tracing applications work and the way they protect the privacy of users can

[1] World Health Organization, (2021) Contact tracing in the context of COVID-19, interim guidance. https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y

create a lack of trust.[2] Hence, concerns and questions related to the privacy of users should be mitigated by the controllers, in order not to hamper the success of the contact tracing applications in the future. Therefore, it is reasonable to assume that such lessons derived from the privacy/data protection law related aspects of Covid-19 digital contact tracing activities can shed light on future use of contact tracing applications, in case that governments will opt for utilizing them again. To this end, the objective of this research is to contribute to the existing data protection law literature by investigating the data protection aspects of contact tracing applications employed within the European Economic Area (EEA, hereinafter),[3] which attracted the most attention due to the nature of the applications, and explores conclusions for the potential future use of contact tracing applications and privacy implications thereof under the European data protection law regime by reviewing the existing literature and the privacy policies and website information of the applications. Accordingly, this article will have a detailed look on the nuances of the European privacy/data protection approach on the applications used by different countries through the following sections.

2. GENERAL FEATURES OF TRACING APPLICATIONS AND THE EUROPEAN UNION PRIVACY FRAMEWORK

With regards to the applicable legal regime for contact tracing applications, establishing a new data protection regime is also time-consuming and rather difficult. Therefore, under the guideline and existing regulations, data controllers endeavor to comply with such requirements. In addition to the General Data Protection Regulation (GDPR, hereinafter)[4] and the ePrivacy Directive,[5] the European Data Protection Board's (EDPB, hereinafter) guideline on the subject was published on April 20, 2020.[6] This guideline and the Commission guideline[7] mutually provide context to the contact

[2] Contact Tracing with Mobile Applications, Tech Dispatch, Issue 1, 2020, p4.
[3] EEA Agreement, Annex XI, Protocol 37, amended by Decision of the EEA Joint Committee No 154/2018, of 6 July 2018.
[4] 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) OJ L 119, 4.5.2016, p. 1–88.
[5] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). O*J L 337, 18.12.2009, p. 11–36*
[6] See European Data Protection Board (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/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en
[7] See eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States 15 April 2020. Available at:

tracing applications from a European perspective on contact tracing matters. As a reflection of the unity that the European Union (EU, hereinafter) wants to provide in a legal sense, there is also the compatibility of laws and guidelines. The Commission took a similar stance on contact tracing applications, referring to the ePrivacy Directive and the GDPR while setting out features and requirements that applications ought to conform to provide compliance with EU privacy and personal data protection legislation, yet the guidance does not cover any further restrictions, such as those that the Member states may have incorporated into their national laws regarding the handling of health data.[8] Therefore, privacy implications of the contact tracing applications should be interpreted by considering each of these regulations, directives and guidelines cumulatively. To put differently, implementing an in-depth analysis of contact tracing applications used within the EEA requires a holistic approach to European privacy regulations and guidance.

Regarding the general features of the applications, the two methods that are used most frequently for digital contact tracing are Bluetooth Low Energy capabilities or GPS location monitoring (Hobson et al, 2020). Pertaining to location-based contact tracing, smartphones can locate themselves using their on-device capabilities (Legendre et al, 2020). Those include GPS for precise location, which, however, mostly works outdoors (+/-2m). As for proximity-based contact tracing, while location-based contact tracing requires an absolute geographical location, technologies such as Bluetooth and Wi-Fi allow inferring the relative proximity of smartphones by transmitting a small-range signal that others can hear and record (up to 50m outdoors and 25m indoors for Bluetooth) (Legendre et al, 2020). In addition, the eHealth Network of the EU advised that location data is not necessary nor recommended for the purpose of contact tracing applications, since their main goal is not to follow the people's movements or to enforce prescriptions.[9] In relation to the collection and processing of the reported data, the divergence between two different types does appear, namely, centralized and decentralized protocols, in which situation protocol corresponds to a standard bunch of rules which enable the phones to communicate with each other.[10] In terms of privacy, both methods (centralized and decentralized) can conform to personal data protection regulations, while the decentralized approach may provide more privacy (Hernández-Orallo, et al., 2020). As per the European Parliament resolution of 17 April, 2020 on EU coordinated action to combat the COVID-

https://health.ec.europa.eu/publications/mobile-applications-support-contact-tracing-eus-fight-against-covid-19-common-eu-toolbox-member_en

[8] 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/?uri=CELEX:52020XC0417(08)

[9] See eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States 15 April 2020. Available at: https://health.ec.europa.eu/publications/mobile-applications-support-contact-tracing-eus-fight-against-covid-19-common-eu-toolbox-member_en

[10] The Association of Schools of Public Health in the European Region (ASPHER), Weitze T, Barros H, Byun. H, (2020) Contact Tracing Apps for COVID-19 An Overview of the European Region, October 2020, p3.

19 pandemic and its consequences (2020/2616(RSP)), decentralized databases for the storage of personal data are required for the data controllers.[11] The decentralized mechanism is preferred by most European countries, and those who opted for a decentralized mechanism utilized DP-3T and the Exposure Notification API by Google and Apple, followed as per the information provided by the European Commission.[12] Nevertheless, the EPDB guideline allows the use of both databases, as long as sufficient security safeguards are provided.[13] We are also supportive of this perspective, as the most crucial part of digital contact tracing activities is to comply with the European standards in place, such as the GDPR,[14] ePrivacy Directive,[15] and related Guidelines published by the EDPB and the Commission.

3. THE EUROPEAN PRIVACY STANDARDS ON TRANSPARENT INFORMATION REQUIREMENT

Providing a privacy statement, thereby informing the users regarding the type, purpose, and nature of the processing activity as well as the storage period of their personal data, is of massive importance for several factors, such as accountability of data controllers[16] as well as a transparent processing[17] as set out in article 5 of the GDPR. Accordingly, the importance of transparent information was stipulated under article 12 of the GDPR.[18] Furthermore, articles 13 and 14 of the GDPR also set out the content of the information to be provided to data subjects.[19] The necessity to include certain types of information in a privacy statement is a GDPR compliance requirement

[11] 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
[12] Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020.
https://health.ec.europa.eu/system/files/2020-07/mobileapps_202006progressreport_en_0.pdf
[13] European Data Protection Board (2020), *op. cit.* p 9
[14] See 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)
[15] 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)
[16] See Article 5-2 of the GDPR, principles relating to processing of personal data, accountability.
[17] See Article 5-1-a of the GDPR, principles relating to processing of personal data, lawfulness, fairness and transparency.
[18] As per article 12 (1) of the GDPR 'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.'
[19] See articles 13 and 14 of the GDPR.

that does not attract as vast attention as the other GDPR requirements (Hintze, 2020). However, transparency requirement always remains significant, specifically in cases in which people have an option as to whether they wish to engage a relationship with a data controller.[20] In case individuals know at the outset what data controllers will use their information for, then individuals can be capable of making an informed choice regarding whether to enter a relationship. For this purpose, to utilize the approach brought by Article 29 Working Party for other processing activities, each data controller should provide information and a confirmation text of a maximum length of one or two pages, concise, transparent, intelligible, and easily accessible.[21] This requirement can be completed with a text that will be required to be read during the first registration phase of contact tracing applications. Accordingly, links to the privacy statement should be indicated in charming locations and in consistent ways across the varied points where an individual data subject interacts with an organization. In its guidance on complying with the GDPR, Article 29 WP, recommended a layered notice to comply with the GDPR requirements that privacy policies be readily available, understandable, and written in plain language.[22] However, above all, it is also important to keep the notices up-to-date and notify the users about the new privacy policies. Even though the importance of being accessible and conceivable was delineated by Article 29 WP, it is still important to transform such requirements into contact tracing applications. The main idea is to implement more frequent reviews on the layered notices than a typical privacy notice provided by an undertaking. To make it more visible to data subjects, once the monthly review of the privacy policies is taken place, data subjects should be notified via different channels not only about the updates but also about the reasoning why such regular reviews on the layered notices and thereby the course of activities of contact tracing applications takes place. We believe that this text should be written in clear, precise, and plain language in line with the spirit of Recital 58 of the GDPR.[23] Also, providing an even shorter text containing only the rights of the data subjects as a box of data under the text to be submitted to the data subjects can play a very serious role in eliminating the problems to be experienced in practice. For contact tracing applications, in the future, each data subject should keep being entitled to exercise their rights both based on legislation in force, and privacy notice provided themselves prior to data processing activities of contact tracing applications, as it is a crucial subject, and might be potentially more widely used going forward, considering that there have been plenty of privacy related arguments in the literature following to the use of the applications.

Furthermore, the GDPR requirements regarding the exercise of data subject rights and the nature of the necessary information meant to place data subjects in a

[20] ICO Website, Guide on Principle (a): Lawfulness, fairness and transparency. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/
[21] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679, p7
[22] *Ibid*.
[23] See Recital 58 of the GDPR.

position where they can assert their rights and hold data controllers accountable for how their personal data is processed.[24] Therefore, for instance, as seen in the case of the Brussels Airport and the use of Thermal cameras[25] to check whether the passengers at Brussels Airport (Belgium) had a body temperature of 38° Celsius or above, the Belgian SA initiated an ex officio investigation against controllers in 2020. Among other things, as per the decision of the Belgian Supervisory Authority, one of the controllers violated Articles 12 to 14 of the GDPR because of a lack of transparency vis-à-vis the data subjects. The fundamental reason of this breach is that the controller's privacy policy did not mention the legal basis for the processing. Hence, as we can see clearly, the privacy policies of contact tracing applications should provide transparency vis-à-vis the data subjects regarding the use of their rights stipulated under the articles 12 to 23 of the GDPR, and we believe that they could be emphasized with short-cut reminders sent as a notification to the mobile phone of the users, whenever they log in.

Furthermore, we are of the view that providing transparency is crucial not only for the accountability of data controllers but also for fostering public trust in the use of contact tracing applications. In other words, the success of any contact tracing application depends on several factors, and we believe that one of the key factors could be the confidence the users have about their privacy and security when using the application. Therefore, data controllers of the applications should also take necessary steps to solidify user trust against any potential privacy risk scenarios. Overall, as detailed in the conclusion part, each of the data controllers located in the GDPR jurisdiction acted accordingly with the transparent information requirement set out in article 12 of the GDPR, and implemented aforementioned necessities precisely. However, it is also important to maintain the high level of transparent communication with data subjects, in line with the current technological developments to sustain this approach successfully in the future.

3.1. Legal basis of the processing activities

Even in situations of emergency, data controllers, including both government and private organizations, are nonetheless governed by the same standard data protection laws (Ventrella, 2020). As a result, it is still imperative that they rely on a legal foundation to ensure the legitimacy of processing operations (Ventrella, 2020). The lawfulness for processing activity was set out under Article 6 of the GDPR, [26,] and Article 9 of the GDPR, considering that digital contact tracing activities contain both special categories of personal data, i.e. health data, and personal data other than special categories. Having said that, in line with the legal grounds set out under the GDPR, the

[24] Guidelines on Transparency under Regulation 2016/679, *op. cit*. p.7
[25] For the full description and decision see: https://edpb.europa.eu/news/national-news/2022/temperature-checks-brussels-airport-belgium-part-fight-against-covid-19_sv
[26] See Article 6 of the GDPR, Lawfulness of Processing states the legal basis of processing.

EDPB indicated its direction by setting forth that where the authorities supply service under a mandate assigned by and in line with requirements stipulated by law, the most appropriate legal basis for the processing seems to be the necessity for the performance of a task in the public interest, namely Article 6(1)(e) of the GDPR. [27] Relevant personal data other than special categories of data may be processed for purposes in accordance with both Article 6(1)(d)[28] and (e)[29] of the GDPR (Ventrella, 2020). While the initial legal ground permits the processing of personal data when it is required to safeguard individuals' vital interests (i.e., to save lives), the second legal justification may be used to safeguard the public interest or in the exercise of official authority granted to the controller.[30] Recital 46 of the GDPR specifically states the monitoring of epidemics as a situation in which the processing may serve both significant bases of public interest and the vital interest of data subjects, public interest can solely be ruled by the law of the Union or of a Member State.[31]

Although consent seems to be the safest option under the GDPR and ePrivacy Directive in many cases for processing special categories of personal data, considering its operational challenges and the urgency of the measures to be taken within the field of public health, the processing does not have to be based on consent as it was provided in article 9-2-I of the GDPR.[32] Hence, public interest and meaningful safeguards plays important role in processing activities. Accordingly, the EDPB's previous statements on imbalance of power between controller and data subjects, also refers to the Recital 43 of the GDPR, which clearly indicates that it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority,[33] which is another supporting reason why consent is not prioritized within the scope of the applications. Accordingly, all of the data controllers of contact tracing applications pay attention to the implementation of the legal basis of the processing activities as per their statements.

For instance, the Spanish Radar Covid application set forth in its assessment to verify the legal basis which established the following:

> *All the information will be collected for purposes strictly of public interest in the field of public health and, in view of the health emergency situation, in order to protect and safeguard an essential interest for people's lives, in the terms outlined in this 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).*[34]

---

[27] European Data Protection Board (2020), *op. cit*. p7.
[28] As per Article 6(1)(d) of the GDPR 'processing is necessary in order to protect the vital interests of the data subject or of another natural person'.
[29] As per Article 6(1)(e) of the GDPR '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'.
[30] *Ibid*.
[31] *Ibid*.
[32] See Article 9-2-I of the GDPR, processing of special categories of personal data.
[33] European Data Protection Board (2020), Guidelines 05/2020 on consent under Regulation 2016/679, p8.
[34] Radar Covid, Privacy Policy, Section 4, para 3 https://radarcovid.gob.es/en/privacy-policy

Similarly, Belgium contact' tracing applications indicated the legal basis of processing activities as follows:

> *The various processing of personal data performed in the framework of this notification process and in the framework of the registration as a user of the Contact Tracing App is based on the grounds of public interest (art. 6.1 (e) GDPR) and, as far as data relating to health are concerned, grounds of public interest in the area of public health (9.2 (i) GDPR). The Contact Tracing App is regulated by the Cooperation Agreement of 25 August 2020. Processing activities are indeed carried out in the public interest as they aim at containing the spread of COVID-19 and protecting the population against this epidemic.'*[35]

Similarly, France's application also established the legal basis of the processing on article 6.1.e of the GDPR,[36] and the Netherlands'[37] application displayed the basis of processing as a public duty. Additionally, many Member state countries, especially Germany,[38] and Estonia,[39] clearly state the type of transactions made based on the collected consents, and the possibility of revoking these consents immediately in case requested by the data subjects, within the scope of the legal basis of processing. Nevertheless, what we would like to point out is that regardless of the choice of the legal basis, there must be a clear and visible unity between the choice of the legal basis for the processing instances within the scope of digital contact tracing activities and their indication to data subjects. Although the countries sampled above, not limited to, opted for different lawful basis for processing activities, they provided their choice of legal basis with an understandable bridge to transparency requirement. Therefore, each of the recommended actions in the Transparency Section could help solidify the indication of the lawful basis as well. Hence, we are of the view that the most important action to implement this lawful basis of the applications is to be clear with the choice of basis and indication thereof. Second of all, determining one dominant legal basis stipulated under Article 6 and 9 of the GDPR, and providing the users of contact tracing applications with it, in addition to other information to be provided to the users, could be an efficient mechanism for the success of the implementation of legal basis. As said, the importance of adopting its own cutting method to indicate these legal bases and acting accordingly during the entire lifecycle of processing activities is of massive importance. For instance, to this end, sending regular SMS and emails related to any change that affects the legal basis of processing activities as also implemented by e-commerce companies, or any need for an update in consent-based transactions could

[35] Corona Alert, Privacy Statement, Section 3, para 1 https://coronalert.be/en/privacy-statement/
[36] Tous Anti-Covid Privacy, Legal Basis and Regulatory Nature of the Processing Section https://bonjour.tousanticovid.gouv.fr/privacy-en.html
[37] Corona Melder, Privacy Policy https://coronamelder.nl/en/privacy
[38] Corona Warn, Privacy, Section 3, para 1 and Section 12, para 1 https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf
[39] HOIA Phone Application Privacy Policy, Section 7, para 1, and Section 13, para 1 https://koodivaramu.eesti.ee/tehik/hoia/app-web/-/blob/master/content/privacy.en.md

be prioritized by data controllers. By these methods, it might be possible to solidify the current application of the lawful basis of the processing by data controllers.

3.2. Data minimization

According to the "data minimization" principle, a data controller should only gather personal data that is directly relevant to and required for the accomplishment of a targeted goal.[40] Additionally, controllers should only store the data for as long as is required to accomplish that goal.[41] During the use of contact tracing applications, European jurisprudence requests to meet criteria such as necessity, proportionality, and data minimization (Vergallo et al., 2021). Pursuant to article 5 of the GDPR, personal data must be relevant, adequate, and restricted to what is needed regarding the purposes for which they are processed.[42] The data minimization principle means that data processing entities enter into a data collection relationship with data subjects only to the extent that is necessary to fulfill processing purposes. Accordingly, the EDPB Guideline 04/2020 also emphasized the importance of data minimization by indicating that applications should not process irrelevant or not needed data, which might include location data, civil status, messages, call device identifiers and so forth.[43] Furthermore, we consider it important to have a holistic approach when assessing the data minimization requirement. In other words, other components of data protection compliance have an impact on implementing an efficient data minimization principle. Accordingly, the outlook of the controllers in Europe is quite positive in this regard. For example, as a good sign of compliance with the GDPR, the Latvian contact tracing application Apturi Covid indicated one of the data minimization implementations thereof in summary by stating, among other things, that the Bluetooth function does not allow processing the user's location data even if the location functionality is enabled in the user's end device.[44] Likewise, the Lithuanian digital contact tracing application declares compliance with the principle of data minimization, by stating that the application was designed to process as little data as possible.[45] Furthermore, the Slovenian application OstaniZdrav clearly indicated the fact that the application will only process the contact data generated and stored by users' mobile phones in case the exposure logging of the application is enabled. [46] As a concrete example of data

[40] EDPS Website, Data Protection Glossary available at: https://edps.europa.eu/data-protection/data-protection/glossary/d_en
[41] *Ibid*.
[42] See Article 5 of the GDPR, Principles relating to processing of personal data.
[43] European Data Protection Board (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, p.9
[44] Apturi Covid Privacy Policy of the App https://apturicovid.lv/documents/apturi-covid-privatuma-politika-en.pdf
[45] Korona Stop Application Privacy Policy https://koronastop.lrv.lt/uploads/documents/files/corona-stop-app/Privatumo-politika-korona-stop-en.pdf
[46] OstaniZdrav Privacy Notice Section 7-b, para 4, available at:

minimization practice in real life, the Icelandic SA determined that it was not essential to obtain the complainant's ID number and birthdate in order to issue him a ticket because the purchase agreement could have been fulfilled without them.[47] As a result, the processing was unlawful and did not adhere to the standards of legality, equity, transparency, and data minimization when handling personal information.[48] We believe that the same logic could be applicable to contact tracing applications. Considering that health data is a wide term and has a broader scope of application, the most convenient way is to limit it to the health data only having a direct relation with Covid-19 pandemic symptoms, and outcomes. In other words, the term strict minimum personal data should not be overstretched by including every information of data subjects related to their healthcare information regardless of its relevancy as the term of "health information" is too broad. Therefore, we think that determining the sub-component of the term health data could be an essential factor to build the data minimization principle thereon. Hence, it is required to create the type and necessity of the information requested by contact tracing applications (Ventrella, 2020). Accordingly, decentralized applications implement data minimization principles and require no user registration as core functions are built into the app (Vuokko et al., 2021). Additionally, such approach could also be implemented by employing strict op-in-mechanism for the data subject to processing, which has secondary importance for contact tracing activities. When users wish to change these settings, they should opt in and amend the settings by themselves. (ex., to share more of their personal data with others) (Calzolaio, 2016). To date, data controllers implement the data minimization principle well, and indicated precisely to its implementation via their privacy policies and website notices. However, as mentioned, it is always possible to solidify the current application of the data minimisation requirements in light of the new technological trends, given that any type of mobile applications now are more reliant on extensive data processing.

3.3. Purpose limitation

The purpose limitation principle is set out under article 5 of the GDPR[49],which obliges data controllers to process data only if it is necessary to process data within the scope of a transaction.[50] Therefore, such transaction must only be limited to the subject of

https://www.gov.si/assets/vlada/Koronavirus-zbirno-infografike-vlada/APP-OstaniZdrav/Privacy-notice.pdf

[47] See EDPB Website News https://edpb.europa.eu/news/national-news/2022/icelandic-sa-fine-imposed-harpa-concert-hall-collection-id-number-and-date_sv

[48] *Ibid*.

[49] See Article 5 of the GDPR, purpose limitation principle.

[50] The European Commission Website, Principles of the GDPR, Purpose of Data Processing https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing_en

that particular transaction between the parties. Similarly, the ePrivacy Directive, detailed the issue of location data collection and explicitly set forth that such a data collection might result in high privacy risks, specifically during movement patterns of individuals being followed (Hatamian et al, 2021). Put differently, whenever a transaction is made, the data controller may process the said data of the data subject only to be limited to that subject. The same logic can provide further implementation context for contact tracing applications. For instance, within the context of contact tracing activities, the purpose of the data processing activity is to prevent the spread of the Covid-19 epidemic 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. Accordingly, the EDPB Guideline 04/2020 also emphasized the importance of purpose limitation principle for the applications by setting out that the purposes should be sufficiently specific to prevent further processing for purposes other than the handling of the COVID- 19 pandemic, such as law enforcement or commercial motives.[51] Therefore, we also believe that data controllers should avoid processing personal data of data subjects whose purpose is not specific enough. From the point of view of the Working Party, a case-by-case analysis is required to determine if further processing for a different purpose could be compatible with the original purpose.[52] Thus, the safest action for contact tracing applications could be to establish a system where data controllers or processors are only able to process the personal data of data subject individuals in society for a clearly defined purpose prior to data processing activities. Hence, the issue of purpose limitation should be interpreted in a very narrow and limited manner by data controllers of the applications, so as not to face any sort of incompliance risk. Digital contact tracing applications should not be used for reasons such as monitoring compliance with quarantine and confinement measures or generalizing about the user's whereabouts (Ventrella, 2020). Similarly, the processing of data to develop novel features and services is not sufficiently specific to comply with this section (Hatamian et al, 2021). To this end, data controllers of contact tracing applications can fulfill such requirements by complying with strict rules from the beginning, as in line with the privacy-by-design principle under the GDPR.[53] Therefore, based on our review, it is reasonable to mention that data controllers of contact tracing applications acted responsibly regarding the implementation of the purpose limitation principle. In general, each of the contact tracing applications provided the purpose of processing in a quite accurate manner. For example, Poland,[54]

[51] European Data Protection Board (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, p.7.
[52] Article 29 Data Protection Working Party Opinion 03/2013, Opinion on Purpose Limitation, P39.
[53] See Article 35-1 of the GDPR, Data protection by design and by default.
[54] StopCovid-ProteGo Documents, Privacy Policy. https://www.gov.pl/web/protegosafe/dokumenty, Section 3, General Rules, Para 2.

Germany,[55] Belgium,[56] Croatia,[57] and the Netherlands'[58] applications clearly indicated the purpose of processing in their privacy notices without causing any ambiguity. We believe that this is a good sign for not facing any arbitrariness in terms of processing for different purposes, and in line with the spirit of the GDPR.

3.4. Technical and organizational measures

Generally, with regard to technical and organizational measures, the integrity, availability, confidentiality, and resilience of the processed data are of massive importance for both data controllers and data subjects. This necessity is set out under Article 5-1-f of the GDPR.[59] As mentioned by the Commission, in general, the degree of security should match the amount and sensitivity of personal data processed.[60] Encryption requirements, IT safeguards, i.e. logical access controls, firewall protections, verification and authentication methods, encryption measures, and so forth, are related safeguards that must be located by each data controller. Not identifiable data should be transmitted with any public or private organization (Bengio et al. 2020). Data that has been pseudonymized or aggregated can be used to construct machine-learning and epidemiological models, as well as to inform public policy. Otherwise, data on users' devices should be encrypted and unavailable to public authorities or private interests. Pseudonymization and anonymization, both of which, are encouraged under the GDPR and enable its constraints to be met.[61] Those retaining personal data ought to implement either of these methods to minimize risk, and automation could diminish the cost of compliance. However, there is a margin to enhance the level of security and technical and organizational measures associated with the data minimization principle. This margin could be filled by establishing state of the art data minimization requirements. Similarly, also advised by the EDPS, EU must take precautions to diligently collect and process the absolute minimum amount of data while utilizing privacy-friendly technology throughout the entire process.[62]

[55] Corona Warn, Privacy *op. cit*. Section 6.
[56] Corona Alert, Privacy Statement *op. cit*. Section 3.
[57] Stop Covid Privacy Notice available at:
https://stopcovid19.zdravlje.hr/html/privacy-policy.html, Section 4
[58] Corona Melder Privacy Policy *op. cit*. Section 2
[59] As per the article 5-1-f of the GDPR 'personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using the appropriate technical or organizational measure.'
[60] Communication from the Commission Guidance on Apps *op. cit*.
[61] GRC World Forums Website, Data masking: Anonymisation or pseudonymisation?. Available at:
https://www.grcworldforums.com/data-management/data-masking-anonymisation-or-pseudonymisation/12.article
[62] EDPS Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis, 2 February 2021, p.10.
https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-manual-contact-tracing-eu_en

Although this guidance deals with European institutions, agencies, and bodies implementing a manual contact tracing system, it might provide further context for digital contact tracing activities as well. Likewise, the EDPB points out the importance of safeguards by setting forth that the contact history or pseudonymous identifiers of a user who has been identified as infected as the result of a thorough assessment by health authorities and a user's voluntary action are the only data that may be collected by a server participating in the contact tracing system.[63]

Correspondingly, each of the data controllers is diligent to implement security safeguards based on their privacy statements. For instance, the Estonian application[64] and Irish application[65] thoroughly indicate the third-party companies involved in the process, while at the same time, the Slovenian application[66] and Lithuanian application[67] display the details of permissions and features the application requires. Likewise, the Czech application mentions the utilization of pseudonymized keys, by stating that the EU, the Ministry, and the users can only access pseudonymized infected person keys sent by the eRouška server.[68] Similarly, the Polish contact tracing application explicitly indicates the methodology for the management of security incidents, including personal data breaches. Additionally, the Croatian application mentioned the usage of random keys, which will only abandon the user's device, if there is any verified infection and only the user approves, so, thereby, it is not possible to establish the relevance between them and the identity of the user.[69] Last but not least, the Italian application shared on the documentation website many important aspects related to the security of the application such as privacy-preserving analytics, security document, and design information with the users.[70] Hence, it is plausible to conclude that this variety of technical and organizational measures have been implemented by data controllers of the applications in line with the goal of mitigating privacy concerns. Nevertheless, data controllers must always be mindful that the nature of the technology and risks could evolve swiftly. Therefore, we believe that it is always diligent to track the technological developments within the field of privacy and interpret the existing requirements under the EU regulations based on these novelties. Such approach would be in line with the essence of the GDPR article 32 of the GDPR setting forth that "solutions should be state-of-art" and "cost efficient".[71]

---

[63] European Data Protection Board (2020), *op. cit*. p9
[64] HOIA Phone Application Privacy Policy *op. cit.* Section 2.
[65] Health Service Executive Application Privacy. Section 9.1.
https://www2.hse.ie/services/covid-tracker-app/data-protection-information-notice.html
[66] OstaniZdrav Privacy Notice *op. cit*. Section 9.
[67] Korona Stop Application, *op. cit*. section 7.
[68] eRouska Application Terms and Conditions and Privacy Policy. Section "Who Has Access Your Data"
https://erouska.cz/en/podminky-pouzivani#osobni
[69] Stop Covid Privacy Notice *op. cit*. Section 7
[70] See Immuni Application Documentation
https://github.com/immuni-app/immuni-documentation#privacy
[71] See Article 32 of the GDPR, security of processing.

4. CONCLUSIONS AND PATH FORWARD

Based on the above-mentioned analyses, data controllers of contact tracing applications employed within the GDPR jurisdictions take their privacy-related responsibilities seriously. What is more, they established a detailed approach to indicate their efforts to users of contact tracing applications. As a positive sign upon the review, each of the data controllers of contact tracing applications tried to act in compliance with the GDPR and other EU guidelines in many aspects based on their privacy policies. To be more specific, for instance, with regards to the voluntary nature of using such applications, we are of the view that the current practice within the EEA has been operated on a strictly voluntary basis, which is compatible with human rights and human psychology. Therefore, it is plausible to state that controllers do respect the Convention,[72] whereas, at the same time, they do not force any citizen on what is deemed contrary to human dignity in the constitutions of the EEA countries. Furthermore, in light of the aforementioned analyses, it is possible to establish some recommendations for a similar future pandemic or infectious disease scenario as well, considering that governments might opt for such applications again, it is always better to be prepared for the privacy-related aspects of such digital contact tracing activities. Given that contact tracing is an important public health safeguard to oversee the spread of infectious disease pathogens, it is plausible to expect that also digital contact tracing could be utilized by the health authorities in future scenarios, as mentioned in the previous sections. Therefore, accordingly, this voluntariness should be maintained and kept indicated to any potential new digital contact tracing activity and privacy policies thereof as well, as it is deemed as one of the key component of the privacy-preserving applications.

Furthermore, although data protection impact assessments (DPIA) already seem sufficient and there was not any serious data breach associated with the utilization of the applications reported, it would be even more privacy-friendly to emphasize the details of the DPIA and selected design approach for each controller, rather than some of them, which could positively impact the perception of the users against any privacy related risk associated with the applications. Similarly, presenting the summary of sufficient guarantees provided by third-party service providers involved in the design and implementation process of the applications could be another key factor for mitigation of any potential data protection/privacy related concerns in the privacy policies of the data controller, which had already been done by many of the controllers. Through this method, any potential concerns related to excessive data storage or a combination of processed personal data for different purposes could be mitigated. Most of the components of data privacy compliance could be considered met as per the website policies of contact tracing applications, and we find their effort successful despite such an urgent and unexpected situation. However, it is always

[72] See Article 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01), protection of personal data.

prudent to implement an anonymous survey in each country to find out potential concerns from a privacy perspective, because perceived risks might be differing from the actual ones in the eyes of the data subjects. Through such activity, it would also be possible to observe the potential feared outcomes associated with the use of such applications, and more privacy-friendly approaches could be derived therefrom. It is also fair to state that data controllers of the contact tracing applications pay significant attention to the implementation of the data minimization principle under the GDPR, considering their indication of using minimum amount of personal data, as per their privacy policies.

In addition, as analyzed in transparency part, given that the applications may change and develop according to the characteristics of the pandemic over time, each update in the notice should be provided to the relevant person in the same way by e-mail and SMS, and the consent requirement for the new update should continue. By this, we are of the view that it would be easier to solidify the trust of users, as data controllers have an opportunity to display the users, that they are taking their duties resulting from the GDPR. Also, as indicated, providing visibility and easy access to the policies for all individuals in society could be an important factor to solidify user trust. Some controllers, in general, locate their privacy statements under the title "privacy policy" at the bottom of their websites in the form of a small tab. However, there is a possibility that it may be ineffective because it is difficult for people to descend to that part, and these parts are not clearly visible. For example, some of the contact tracing applications have a privacy policy as a big and separate tab at the entrance of their websites, which is an efficient method to emphasize the importance of privacy features of the applications. The same logic could be utilized for the any potential future applications as well.

Last, but not least, mitigating the inherent risks in their source is of key to success of data controllers in their compliance efforts. Therefore, it is important to establish a strong privacy by design and default approaches as set out under the GDPR.[73] Complying with the principles of successful data protection and privacy by design is important to persuade target populations to download and use digital contact tracing applications (O'Connell et al., 2021). Embedding GDPR requirements into the designed application could drastically reduce the risk of breach of the GDPR requirements. Therefore, to summarize, applications used in the GDPR jurisdictions implemented privacy requirements thoroughly, but it is always important to enhance such compliance activities, in light of the latest technologies going forward. Thus, for any potential future use of such apps, data controllers will be able to benefit both from their experience with the current situation and further studies in the field of privacy aspects of contact tracing applications.

[73] See Article 25 of the GDPR, data protection by design and default.

LIMITATIONS

While elaborating on these features regarding the compliance efforts of data controllers with the European privacy laws and guidelines, it is important to note that these conclusions must be supported by further studies regarding the trust of the users and the creation of statistical data regarding the correlation between compliance requirements and user trust. The outcomes derived in this article is limited to the existing relevant literature and the website privacy policies of contact tracing applications.

ACKNOWLEDGEMENT

Raif Baran Tombul thanks Prof. Antoni Roig Batalla for his constant support during the research.

REFERENCES

Bibliography

Bengio, Y. (et al.) (2020). A. The need for privacy with public digital contact tracing during the COVID-19 pandemic. *Lancet Digit Health*, *2*(7), p. e342-e344. https://doi.org/10.1016/S2589-7500(20)30133-3

Blasimme, A.; Ferretti, A. and Vayena E (2021). Digital Contact Tracing Against COVID-19 in Europe: Current Features and Ongoing Developments. *Frontiers in Digital Health,* 3:660823. https://doi.org/10.3389/fdgth.2021.660823

Calzolaio, S. (2016). Digital (and privacy) by default. Constitutional identity of e-government. *Giornale di Storia Costituzionale*, *31*, p, 185. http://www.storiacostituzionale.it/doc_full-text/GSC_31_full-text.pdf

Hatamian, M., Wairimu, S., Momen, N. & Fritsch, L. (2021). A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical software engineering*, 26, 36. https://doi.org/10.1007/s10664-020-09934-4

Hernández-Orallo, E.; Calfate, C.T.; Cano, J.C.; Manzoni, P. (2020). Evaluating the effectiveness of COVID-19 Bluetooth-Based smartphone contact tracing applications. *Applied Sciences, 10* (20). https://doi.org/10.3390/app10207113

Hintze, M. (2019). Privacy Statements under the GDPR. Seattle University Law Review, *42*(3). https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/7/

Hobson, S.; Hind, M.; Mojsilovic, A. and Varshney, K.R. (2020). Trust and transparency in contact tracing applications. *arXiv:2006*, 11356. https://doi.org/10.48550/arXiv.2006.11356

Legendre, F.; Humbert, M.; Mermoud, A.; Lenders, V. (2020). Contact tracing: An overview of technologies and cyber risks. *arXiv:2007*, 02806. https://doi.org/10.48550/arXiv.2007.02806

Mbunge, E (2020). Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. *Diabetes & Metabolic Syndrome*, *14*(6). https://doi.org/10.1016/j.dsx.2020.08.029

O'Connell, J. (et al.) (2021). Best practice guidance for digital contact tracing apps: a cross-disciplinary review of the literature. *JMIR mHealth and uHealth*, *9*(6). https://doi.org/10.2196/27753

Scantamburlo, T. (et al.) (2021). Covid-19 and tracing methodologies: A lesson for the future society. *Health and Technology*, 11,.pp. 1051–1061. https://doi.org/10.1007/s12553-021-00575-1

Ventrella, E. (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

Vergallo, G. M.; Zaami, S. and Marinelli, E. (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*, *25* (5), pp. 2449-2456. https://doi.org/10.26355/eurrev_202103_25286

Vuokko, R.; Saranto, K. and Palojoki, S. (2021). Features of COVID-19 applications and their impact on contact tracing: results of preliminary review. *Finnish Journal of eHealth and eWelfare*, *13*(4). https://doi.org/10.23996/fjhw.109253

Official documentation

Application #OstaniZdrav. *Privacy notice*. https://www.gov.si/assets/vlada/Koronavirus-zbirno-infografike-vlada/APP-OstaniZdrav/Privacy-notice.pdf

Apturi Covid Privacy Policy. https://apturicovid.lv/privatuma-politika/#en

Article 8 of the Charter of Fundamental Rights of The European Union (2000/C 364/01), protection of personal data. https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#:~:text=1.,basis%20laid%20down%20by%20law

Article 29 Data Protection Working Party. Opinion 03/2013, Opinion on Purpose Limitation. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Working Party Guidelines on Transparency under Regulation 2016/679. https://gdpr-text.com/guidelines/transparency/

Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01. OJ C 124I, 17.4.2020, p. 1–9. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)

Corona Melder. *Privacy Policy*. https://coronamelder.nl/en/privacy

Corona Warn App. *Privacy Notice Version 3.2*. https://www.coronawarn.app/assets/documents/cwa-privacy-notice-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, 19.7.2018, p. 23–26*. https://eur-lex.europa.eu/eli/dec/2018/1022/oj

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). OJ L 201, 31.7.2002, p. 37–47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the

enforcement of consumer protection laws (Text with EEA relevance). OJ L 337, 18.12.2009, p. 11–36. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0136

eHealth Network. *Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States. Version 1.0. 15 April 2020*. https://ec.europa.eu/health/system/files/2020-04/covid-19_apps_en_0.pdf

eRouska. *Terms and Conditions and Privacy Policy*. https://erouska.cz/en/podminky-pouzivani#osobni

European Centre for Disease Prevention and Control (28 Jun 2022). *Considerations for contact tracing during the monkeypox outbreak in Europe*. https://www.ecdc.europa.eu/en/publications-data/considerations-contact-tracing-during-monkeypox-outbreak-europe-2022

European Comission. *Mobile applications to support contact tracing in the EU's fight against COVID-19 Progress reporting June 2020*. https://health.ec.europa.eu/system/files/2020-07/mobileapps_202006progressreport_en_0.pdf

European Commission. *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

European Data Protection Board. *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*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

European Data Protection Board. *Guidelines 05/2020 on consent under Regulation 2016/679*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

European Data Protection Board (2022). *Temperature checks at Brussels Airport (Belgium) as part of the fight against COVID-19* https://edpb.europa.eu/news/national-news/2022/temperature-checks-brussels-airport-belgium-part-fight-against-covid-19_sv

European Data Protection Supervisor. *TechDispatch #1/2020. Contact tracing with mobile applications*. https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en

European Data Protection Supervisor. *Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis, 2 February 2021*. https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-manual-contact-tracing-eu_en

European Data Protection Supervisor. *Glossary*. https://edps.europa.eu/data-protection/data-protection/glossary_en

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

France. MinIstère de la Santé et de la Prévention (2022). *TousAntiCovid*. https://bonjour.tousanticovid.gouv.fr/privacy-en.html

Gobierno de España. *Privacy policy of the Radar Covid Application*. https://radarcovid.gob.es/en/privacy-policy

Gov. Poland. *Stop Covid Documenty*. https://www.gov.pl/web/protegosafe/dokumenty

GRC World Forums. *Data masking: Anonymisation or pseudonymisation?*. https://www.grcworldforums.com/data-management/data-masking-anonymisation-or-pseudonymisation/12.article

Health Service Executive. *COVID Tracker App: Data Protection Information Notice (DPIN)*. https://www2.hse.ie/services/covid-tracker-app/data-protection-information-notice.html

HOIA Phone Application Privacy Policy. https://koodivaramu.eesti.ee/tehik/hoia/app-web/-/blob/master/content/privacy.en.md

IAPP. *Layered Notice*. https://iapp.org/resources/article/layered-notice/

Information Commissioner's Office (ICO). *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/

Immuni App. Privacy.
https://github.com/immuni-app/immuni-documentation#privacy

Korona Stop LT' Privacy Policy.
https://koronastop.lrv.lt/uploads/documents/files/corona-stop-app/Privatumo-politika-korona-stop-en.pdf

Privacy Statement. *Contact Tracing App – Belgium. Corona Alert, 14 April 2022*.
https://coronalert.be/en/privacy-statement/

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).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Smitte stop (Denmark). *Processing of Personal Data*. https://smittestop.dk/en/data-protection/

Stop Covid-19 Exposure notifications. *Privacy notice*.
https://stopcovid19.zdravlje.hr/html/privacy-policy.html

The Association of Schools of Public Health in the European Region (ASPHER). *Contact Tracing Apps for COVID-19. An Overview of the European Region. October 2020*.
https://www.aspher.org/download/521/contact-tracing-apps-for-covid-19-an-overview-of-the-european-region.pdf

World Health Organization (2021). *Contact tracing in the context of COVID-19. Interim guidance*.
https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y

World Health Organization (2022). *Surveillance, case investigation and contact tracing for mpox (monkeypox): interim guidance.*
https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_402e2db4-d306-4ff6-a386-e990da186971