CHALLENGES OF PROCESSING PERSONAL DATA IN THE CONTEXT OF THE COVID-19 PANDEMIC

Mathias Cardarello Fierro[*]

Cybersecurity and Privacy Preservation Techniques and Digital Security and Privacy
Master in Data Science and Economics

24 Nov 2021

ABSTRACT

The COVID-19 global health crisis led governments to adopt privacy-invasive measures to mitigate the spread of the pandemic. In particular, the widespread use of contact tracing apps has tested the data protection and privacy frameworks such as Europe's General Data Protection Regulation (GDPR). We analyse the compatibility of the contact tracing solutions applied by EU Member States with privacy and data protection regimes and principles, finding that most of them followed the EU guidelines and recommendations.

Keywords: contact tracing, COVID-19, data protection, EU, GDPR, privacy, public health.

TABLE OF CONTENTS

[*]Università degli Studi di Milano.

INTRODUCTION

The outbreak of the COVID-19 pandemic in late 2019 resulted not only in a global health crisis but also in a challenge to the resilience of data protection principles, due to the rapid digitalisation of every aspect of our lives. Privacy-invasive measures adopted by governments and organisations include questioning individuals about their travel plans, processing location data, performing temperature checks and keeping health records together with information about the possible contact with infected individuals. The majority of them are related to one of the most vulnerable categories of data, health data, therefore privacy and data protection are critical in their rollout.

In particular, the development of contact tracing applications was the most important effort made by governments to gather information as quickly and efficiently as possible to address COVID-19. Although "data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake"[1], there is a fine line between safety measures benefiting public health and invasive controls that affect the privacy of people.

The widespread use of contact tracing apps, which track individual movements and their health status using digital exposure notification systems, has tested the data protection and privacy frameworks such as Europe's General Data Protection Regulation (GDPR). Indeed, according to the report *"Privacy and Data Protection in the age of COVID-19"* (Deloitte, 2020), "the current global health crisis is the first real obstacle the GDPR has to overcome since it came into force" in May 2018.

In this article, we examine the compatibility of the contact tracing solutions applied by European Union (EU) members with privacy and data protection regimes and principles, in particular, the Convention 108+ and the GDPR.

I. REGULATORY FRAMEWORK

In the EU, the GDPR provides the main legal architecture for the handling and processing of personal data "in order to be lawful, fair, and reflecting the underpinning social and ethical values of the European Union" (Christofidou et al., 2021). Furthermore, Convention 108 and the actualised "Convention 108+" set forth high standards for the protection of personal data which are compatible with other fundamental rights and public interests. More recently, two statements were adopted at EU level in the context of the COVID-19 outbreak. On 16 March 2020, the chair of the European Data Protection Board (EDPB)

[1] Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, available at https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

issued a formal statement on the processing of personal data and, on 30 March 2020, the European Data Protection Supervisor (EDPS) replied to the European Commission concerning about monitoring the spread of the COVID-19 outbreak.

In the following subsections, we present a brief description of the data protection and privacy frameworks previously mentioned.

A. Convention 108 and Convention 108+

The Convention for the Protection of Individuals with regard to Automated Processing of Personal Data, also known as "Convention 108", has served as the foundation for international data protection law in European countries. Being opened for signature on 28 January 1981 by the Council of Europe (CoE), it has also influenced policy and legislation beyond European countries. To deal with challenges resulting from the use of new information and communication technologies, the CoE started in 2011 a process to update the Convention and, on 10 Oct 2018, the "Convention 108+" was opened for signature.

One of the main data protection principles provided by Convention 108+ is the principle of lawfulness, according to which processing of data can be carried out based on the data subject's consent or some other legitimate basis defined by law. More specifically, according to Article 11, exceptions shall be

> "provided for by law, respect the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society".

Where restrictions are being applied, such as in the case of monitoring the COVID-19 pandemic, those measures have to be taken on a provisional basis and only for a limited period.

Following Convention 108+ it is crucial that, even in particularly emergency situations, data protection principles are respected. Therefore, it must be ensured that data subjects are aware of the processing of personal data related to them and they are entitled to exercise their rights, only necessary and proportionate personal data is processed, the specified and legitimate purpose is pursued, an impact assessment is carried out before the processing is started, privacy by design[2] is ensured, and appropriate measures are adopted to protect the security of data.

[2]Privacy by design means building privacy into the design, operation, and management of a given system, business process, or design specification. This means that data protection in data processing procedures is best adhered to when it is already integrated with the technology when created.

B. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the EU. It was adopted on 14 April 2016 and became enforceable beginning 25 May 2018.

GDPR establishes responsibilities for organisations to ensure the privacy and protection of personal data, defined in Article 4 § 1 as

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly (...)"

from that data, provides data subjects with certain rights, and assigns powers to regulators to ask for accountability or even impose fines in cases where an organisation is not complying with the requirements.

The COVID-19 outbreak was seen as a challenge to the GDPR and how governments and organisations process personal data to mitigate the spread of the pandemic, particularly through two types of measures implemented. On the one hand, through the exemptions used by the public institutions provided under Article 9 § 2 to enable health data to be used for research purposes:

> "(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

On the other hand, through the use of mobile applications aimed to track the movements of the citizens and collect data about their health status.

As it was expressed by the Belgian Data Protection Authority on March 2020, processing of personal data in the context of COVID-19 must comply with all the fundamental principles of data processing of Article 5 of the GDPR:

1. Lawfulness, fairness and transparency: Processing must be lawful, fair, and transparent to the data subject.

2. Purpose limitation: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

3. Data minimization: You should collect and process only as much data as absolutely necessary for the purposes specified.

4. Accuracy: You must keep personal data accurate and up to date.

5. Storage limitation: You may only store personally identifying data for as long as necessary for the specified purpose.

6. Integrity and confidentiality: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).

7. Accountability: The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

However, rather than being an obstacle, the principles-based approach of the GDPR is viewed as a "functional blueprint for systems design that is compatible with fundamental rights" (Bradford et al., 2020), such as the protection of personal data, an advantage in conditions of uncertainty.

C. European Data Protection Board (EDPB) statement

The "Statement on the processing of personal data in the context of the COVID-19 outbreak", adopted by EDPB on 16 March 2020 and updated three days later, highlights that data protection does not form a barrier to public health in exceptional times. Although stating that

> "emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period",

a number of considerations are necessary to assure the lawful processing of personal data. Therefore, both data controller and processor must ensure the protection of the personal data of the data subjects.

In particular, employers and public health authorities do not have to rely on the individual's consent to process personal data in the context of a pandemic but can rely on Article 6 (Lawfulness of processing) and Article 9 (Processing of special categories of personal data) of the GDPR. The EDPB also states that when localisation data is being processed, national laws implementing the e-Privacy Directive[3] must also be respected. Finally, the EDPD highlights that national legal restrictions have to be considered when processing personal data in the employment context.

[3]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).

D. European Data Protection Supervisor (EDPS) statement

On 30 March 2020, the EDPS released the "Joint Statement on the right to data protection in the context of the COVID-19 pandemic", in which it was stressed that

> "States have to address the threat resulting from the COVID-19 pandemic in respect of democracy, rule of law and human rights, including the rights to privacy and data protection."

In this document, the EDPS commented on general data protection principles and rules, under Convention 108+, processing of health-related data, based on the Recommendation CM/Rec(2019)2 of the Council of Europe[4], large-scale data processing, data processing by employers, as stated in the Recommendation CM/Rec(2015)5 of the Council of Europe[5], and data processing in educational systems.

In particular, the EDPS advised the European Commission to apply to third parties equivalent security measures and strict confidentiality obligations and prohibitions regarding data security and data access. However, data that was effectively anonymised fall outside of the scope of data protection rules. Furthermore, the EDPS stressed that the data obtained through digital devices should be deleted as soon as the health emergency finishes, in line with Article 11 of Convention 108+:

> "Where restrictions are being applied, those measures have to be taken solely on a provisional basis and only for a period of time explicitly limited to the state of emergency".

II. Contact tracing apps: Impact on data protection rights

Among the measures undertaken to fight against the COVID-19 pandemic, many EU countries have developed contact tracing applications to monitor citizen movements and push notifications to their mobile phones, using the so-called digital exposure notification system. This technology, a new version of the traditional contact tracing processes that help stop the spread of a virus, have led to significant legal implications for the privacy and freedoms of individuals.

This section explores the impact on privacy and data protection rights of European digital contact tracing solutions, and it is organised as follows. In the first subsection, we

[4]Recommendation CM/Rec(2019)2 of the Committee of Ministers to Member States on the protection of health-related data (Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies).

[5]Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies).

present a summary of the EU guidelines and recommendations regarding the development of contact tracing apps. Next, we briefly describe the specific national legislative measures for data collection in these apps. Finally, we analyse the data subjects' rights implications of COVID-19 tracing systems deployed by EU members, concerning the data protection and privacy frameworks aforementioned.

A. EU guidelines

The deployment of contact tracing applications has been prioritised among COVID-19 containment measures in the EU, where most countries have launched their national version. In this context, on 8 April 2020, the European Commission issued Recommendation 2020/5189[6], proposing a common approach to the use of mobile applications and mobile data in response to the coronavirus pandemic across the EU Member States.

The purpose of the Recommendation was to support the gradual lifting of coronavirus containment measures by using data retrieved from mobile apps and provided key principles for their use in the context of social distancing measures, for warning, prevention and contact tracing. The Recommendation was followed by the "Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection"[7], which sets out the features and requirements apps should meet to ensure compliance with EU privacy and personal data protection legislation.

In summary, the framework developed by the Commission provides that tracing apps must be voluntary, transparent, temporary, cybersecure, and use temporary and anonymised data. They should rely on Bluetooth proximity technology that does not enable the tracking of people's locations, instead of the more privacy-invasive GPS, be approved by national health authorities, and should guarantee interoperability across borders and mobile operating systems. The Commission also highlighted that any use of apps and data must respect data security and EU fundamental rights, such as privacy and data protection.

B. Specific national regulations

Although the majority of Data Protection Authorities (DPA) of the EU Member States have been involved in the development of COVID-19 apps, only a few countries set up specific legislation and followed the preliminary steps to limit the impact of the tool on fundamental rights, as required by the e-Privacy Directive. According to Article 15 § 1, the

[6]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.

[7]Communication from the Commission Guidance of 17 April 2020 on Apps supporting the fight against COVID 19 pandemic in relation to data protection.

exceptional national legislative measures can restrict the scope of the rights and obligations provided by the regime

> "(...) when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society (...)".

Only the governments of Belgium, Finland, France, Italy and Norway passed legislation to regulate contact tracing apps. In particular, the Italian government incorporated into legislation a set of safeguards, such as that the app should be voluntary and based on Bluetooth data, that personal data should not be used for other purposes, unless anonymised and used only for statistical purposes once the purpose of their transmission is achieved, among others. The Finnish regulation provides a specific legal basis and appropriate GDPR safeguards for the tracing app, while the proposed law in Belgium requires that apps should not trace the user all the time.

C. Evidence from the experiences in the EU

While most EU countries developed apps to detect proximity and contact tracing, some others focused on apps aimed at fulfilling other purposes, such as giving information to the population, medical support and crowd control.

Regarding tracing apps, various protocols[8] have been developed since the beginning of the health crisis, providing different functionalities. There are two different approaches, the centralised data collection by the national authorities, and the decentralised data processing. In the centralised approach, all proximity data are exclusively calculated and processed in the app. The European Commission and the EDPB did not back a specific approach, but the European Parliament recommends the use of decentralised models. During the discussion about which system is the best, the issues most highlighted regarding privacy and data protection were the risk of "function creep"[9], identification of data subjects or vulnerability to cyberattacks, with centralised systems attracting particular concern.

In the majority of the EU Member States, contact tracing apps were developed under a decentralised approach, such as Austria, Cyprus, Estonia, Finland, Germany, Ireland, Latvia, Poland and Portugal. In some countries, health authorities can only have limited access to data from users (Estonia, Finland and Poland). However, in Belgium, Bulgaria, Czechia, Denmark, France, Italy, Lithuania, Slovakia and Spain, a centralised approach was applied, therefore data is stored and processed on a central server.

Furthermore, most EU governments have deployed COVID-19 apps that use Bluetooth to trace all COVID-19 positive contacts of device users, estimating their proximity only

[8] In mobile devices, a protocol establishes the set of rules determining how the data will be transmitted.

[9] "Function creep" occurs when information is used for a purpose that is not the originally specified purpose.

based on signal intensity. This technology has a privacy advantage over GPS based data because the only information it involves is anonymised contact tokens, which can be cryptographically secured because is less vulnerable to deanonymisation than location data. With this alternative, governments have found an appropriate balance between data privacy and the public interest, following the recommendations of the European Commission and the EDPB as well. However, apps in Bulgaria, Cyprus and Lithuania are based on network or GPS location data, while in Slovakia the available app uses both technologies.

Another important aspect that was mentioned for the protection of privacy and personal data processing is the free availability of the app code. In the 2020 Data Protection Report of the CoE, it was stated that:

> "The publication of the source code help to build confidence in the system, as an important aspect of transparency, and provides means of control of the respect for the rights to privacy and data protection."

According to a study of the European Union Agency for Fundamental Rights (FRA)[10], most EU member States made available the source code of tracing apps, promoting transparency in personal data processing.

However, several government measures were criticised and put in debate for not respecting data protection rules. In Bulgaria, for example, the Constitutional Court ruled that the legislative amendment allowing access to traffic data about individuals in mandatory isolation was unconstitutional, as the six-month period for retaining their data was excessive. In Croatia, proposed legal amendments to track the location of people in self-isolation were eventually withdrawn.

Furthermore, in Germany and the Netherlands, there was a public debate about the privacy risks of contact tracing apps. In Germany, for instance, the development of the app was critically followed by the federal DPA that did not see any objection against its use. Intending to tackle data protection issues, Germany and other 16 EU countries conducted a Data Protection Impact Assessment (DPIA), although not all are publicly available.

CONCLUSIONS

As previously stated, the COVID-19 pandemic was a great challenge for the adaptability of the regulations on privacy and personal data protection in an emergency context. Due to the urgent need to collect data from individuals about their health and contact exposure, it was expected that fundamental rights would have to be balanced against each other.

[10]Coronavirus pandemic in the EU: fundamental rights implications. Bulletin 2, 21 March - 30 April 2020.

Although several EU Member States measures were criticised for not respecting some data protection rules, the majority of them followed the EU guidelines and recommendations regarding the development of contact tracing apps.

The health crisis also challenged the effective functioning of democracies, in which data protection rights are a key component. The compliance with the legal framework and the cooperation between policymakers and stakeholders involved in the fight against the pandemic, including civil society, increase the trust and acceptance of citizens of the measures adopted in the general interest. Public debates, publication of the tracing application codes and the conduct of DPIA were the main tools that boosted public support.

Moreover, given the evidence from EU Member States on the processing of personal data in the context of COVID-19, in particular through contact tracing applications, there is a clear need for a more harmonised approach that may result in more efficient responses to future emergencies.

REFERENCES

[1] Bradford, L., Aboy, M., Liddell, K. (2020). *COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes.* Journal of Law and the Biosciences, 7(1), lsaa034.

[2] Christofidou, M., Lea, N., Coorevits, P. (2021). *A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis.* Yearbook of Medical Informatics, 30(01), 226–232.

[3] *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Treaty Series-No. 223). (n.d.). Council of Europe.

[4] *2020 Data Protection Report.* (2020). Council of Europe.

[5] *Privacy and Data Protection in the age of COVID-19. Fundamental questions and considerations.* (2020). Deloitte.

[6] European Union Agency for Fundamental Rights. (2020). *Coronavirus pandemic in the EU: Fundamental rights implications. Bulletin 2, 21 March - 30 April 2020.* Publications Office.

[7] European Union Agency for Fundamental Rights. (2021). *Fundamental Rights Report 2021.* Publications Office.

[8] Jelinek, A. (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak.* European Data Protection Board.

[9] Kedzior, M. (2021). *The right to data protection and the COVID-19 pandemic: The European approach.* ERA Forum, 21(4), 533–543.

[10] Pierucci, A., Walter, J.-P. (2021). *Joint Statement on the right to data protection in the context of the COVID-19 pandemic.* Council of Europe.

[11] Rana, O., Llanos, J., Carr, M. (2021). *Lessons from the GDPR in the COVID-19 era.* Academia Letters.

[12] *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), (2016).

[13] Rosenberger, A., Shvartzshnaider, Y., Sanfilippo, M. (2021). *Digital Contact Tracing in the EU: Data Subject Rights and Conflicting Privacy Governance.* Proceedings of the Association for Information Science and Technology, 58(1), 819–821.