TRACKING AND TRACING APPS AND DATA PROTECTION IN THE CONTEXT OF THE COVID-19 PANDEMIC

DATA PROTECTION REQUIREMENTS AND RECOMMENDATIONS
FOR THE DEPLOYMENT OF COVID-19 TRACKING AND TRACING APPS.

FRANZISKA BOEHM, DIANA DIMITROVA, FRANCESCA PICHIERRI AND DARA HALLINAN[1]

April 2020

INTRODUCTION

Since the outbreak of the COVID-19 pandemic, countless apps have been developed worldwide, which collect pandemic-relevant data. The data collected ranges from anonymised location data to sensitive health data. Medical professionals believe the use of these apps is appropriate, even necessary, in order to ensure the long-term containment of the pandemic. Politicians discuss whether they should recommend the voluntary use of the apps to citizens. We will soon face difficult choices concerning whether we want to install such apps and if so, which apps we want to install.

The reason for this is: according to their goal and purpose, apps are designed differently, and, as a result, their differing functions represent different degrees of invasiveness into the rights of users. Some apps serve to inform users about other individuals who have had contact with COVID-19 sufferers, other apps aim to support research and yet other apps aim to ensure compliance with lockdown rules.

All apps, with differing degrees of emphasis, have the protection of public health as their main goal. However, all uses are also fraught with risks for the right to the protection of personal data and their effects on this right should be carefully balanced against possible benefits. Consequently, all individuals who are considering using an app, can only make an informed decision concerning the pros and cons of use if they are aware of the advantages, as well as the disadvantages, in advance.

It will be a political task to ensure this transparency and to recommend apps which require the minimum possible infringement of the users' rights as well as the optimum balance between users' rights and the protection of public health. Otherwise a serious loss of trust may occur, reflecting a perception that the use of apps implies a disproportionate infringement of rights. In this regard, app-developers, and their data protection officers, are called upon to design apps which recognise the need for an appropriate balance between users' rights and public health.

To provide an initial orientation for how this might be achieved, we have analysed the prerequisites, in EU law, which must be fulfilled by COVID-19 tracking and tracing apps and, on the back of this analysis, have elaborated a series of data protection recommendations for app design and deployment.

In the analysis, we also investigated the degree to which seven apps, all recently deployed in EU Member States, conform to data protection law requirements. The provisional findings concerning these apps are outlined in two specifically designed and conceptualised tables. These findings will be updated as apps are further developed, and as new information becomes available.

1 Prof. Dr. Franziska Boehm is Head of the Intellectual Property Rights department at FIZ Karlsruhe and holder of the Professorship of the same name at Karlsruhe Institute for Technology (KIT). Diana Dimitrova, Dr. Dara Hallinan and Francesca Pichierri are researchers in the Intellectual Property Rights department.

TABLE OF CONTENTS

I. GENERAL CONDITIONS FOR DATA PROCESSING

1. LEGAL BASIS – ARTICLE 6 GDPR

Whenever personal data are processed, Article 6 GDPR applies. According to Article 6, the processing of personal data is **lawful only if**:

- the data subject has given consent to the processing of his or her personal data (Article 6(1)(a) GDPR). Consent must be informed, freely given, unambiguous and specific.[2]
- the processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6(1)(c) GDPR). For example, an employer could be subject to a legal obligation relating to health and safety in the work-place.[3]
- the processing is necessary to protect vital interests of the data subject or of another natural person (Article 6(1)(d) GDPR). The "monitoring of epidemics and their spread" is explicitly mentioned in Recital 46 GDPR as vital interest. Data can be processed in order to protect both infected people and others, to prevent them from being infected;[4]
- the 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 (Article 6(1)(e) GDPR). This legal basis will usually be invoked by public authorities and such a measure should be based on a national implementing law (Article 6(2) GDPR);
- if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(f) GDPR) and where the interests of the controller do not outweigh those of the data subject;[5]

2. LEGAL BASIS – ARTICLE 9 GDPR

When special categories of personal data, such as **data concerning health, genetic data or biometric data**, are processed, **Article 9 GDPR** has to be respected. For example, COVID-19 tracking apps may process sensitive information about the symptoms a person is experiencing such as shortness of breath or dry cough, pre-existing medical conditions, facial expressions or contacts with confirmed positive patients. The latter could be considered to be sensitive personal data, because the fact that someone had contact with an infected person could mean that he is potentially also infected and poses a disease risk. Information connected with disease risk is explicitly mentioned as data concerning health in Recital 35 GDPR.[6] The GDPR foresees exceptions to the prohibition of processing of special categories of per-

2 See Article 29 Working Party, "Opinion 15/2011 on the notion of consent", WP 187, July, 2011.

3 See European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

4 See Christina Etteldorf, "COVID-19Special: EU Member State Data Protection Authorities Deal with COVID-19: An Overview," EDPL (2) 2020, p. 3, available at https://www.lexxion.eu/wp-content/uploads/2020/03/COVID-19-Special-Data-Protection-Authorities-Deal-with-COVID-19.pdf; see also Christopher Kuner and Massimo Marelli, "Handbook on Data Protection in Humanitarian Action", August 2017, available at file:///C:/Users/FPI/Downloads/4305_002_Data_protection_and_humanitarian_action_low.pdf; Dara Hallinan and Frederik Zuiderveen Borgesius, "Article 6" in Franziska Boehm and Mark Cole (eds.), GDPR Commentary (Elgar, Forthcoming).

5 Article 6(1) (f) 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 re-pealing Directive 95/46/EC (General Data Protection Regulation), (2016) OJ L119/1, (GDPR), does not apply to processing carried out by public authorities in the performance of their tasks; these authorities have to rely on Article 6(1)(e) GDPR. See also Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", 09 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

6 The breadth of the definition of data concerning health will mean that Covid-19 apps will likely usually process data concerning health.

sonal data where for example the data subject explicitly consents to the data processing (Article 9 (2) (a)); the processing is necessary for reasons of substantial public interest (Article 9 (2) (g)); the 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 (Article 9 (2) (h); the processing is necessary for reasons of substantial public interest in the area of public health (Article 9 (2) (i)), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Article 9 (2) (c)), as Recital 46 GDPR explicitly refers to the control of an epidemic (as seen above).

In particular, Article 9 (2) (i) GDPR could be relied on for the processing of sensitive data in the framework of the current COVID-19 pandemic because it allows the processing of sensitive data to protect against "serious cross-border threat to health".[7] The recent Latvian DPA (the DVI)'s guidelines, issued in the context of the COVID-19 health emergency, underline that Article 9(2)(j) GDPR could be a legal basis for **scientific research purposes** or statistical purposes as well.[8]

3. PROCESSING OF LOCATION DATA – ePRIVACY DIRECTIVE

When telecoms data, such as location data, are processed, national laws implementing the ePrivacy Directive must also be respected. Using mobile location data is a possible way to monitor or contain the spread of COVID-19. This may involve, for instance, the possibility to geo-locate individuals or to send public health text-messages to individuals in a specific geographical area. As stated by the European Data Protection Board (EDPB), "in principle, location data can only be used by the operator when made anonymous or with the consent of individuals".[9] According to Article 5 (3) ePrivacy Directive, for any usage of a mobile application, without distinction as to whether the information is personal data or not, the consent of the end-user is needed.[10] However, the EDPB also notices that "Article 15 of the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security".[11] The EDPB elaborates that "such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention on Human Rights. Moreover, it is subject to the judicial control of the European Court of Justice and the European Court of Human Rights".[12] Further, emergency measures must be "**strictly limited to the duration of the emergency at hand**".[13]

7 Article 9 (2) (i) GDPR.
8 See GDPR Hub, "Data Protection under SARS-CoV-2," available at https://gdprhub.eu/index.php?title=Data_Protection_under_SARS-CoV-2.
9 European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020, p. 2, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.
10 Article 5 (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), OJ L 201, 31.7.2002 as amended by Directive 2009/136/EC of the European Parliament and of the Council, 25 November 2009, OJ L 337/11, 18.12.2009.
11 European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020, p. 2, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.
12 Ibid.
13 Ibid.

4. PRINCIPLES OF DATA PROCESSING – ARTICLE 5 GDPR

Data processing activities must comply with the principles of data processing established by Article 5 GDPR.[14] Data processing must be **lawful** under Article 6 GDPR and/or Article 9 GDPR, as well as under any other laws applicable to the processing in question.[15] Some member states have already adopted laws which concerns the COVID-19 emergency. These laws must be taken into consideration when assessing the lawfulness of processing. Furthermore, processing must be **fair and transparent**. The principle of fair processing guides the relationship between the data subject and the controller. The latter should notify data subjects that they will process data in a lawful and transparent manner. Processing operations should not be performed in a secret or misleading way. Data controllers have to make it possible for data subjects to "really understand what is happening with their data"[16] (including to inform them of any potential risks connected with the processing) and should act in a way which takes into account the legitimate expectations of the data subjects. The "principle of fairness goes beyond transparency obligations and could also be linked to processing personal data in an ethical manner".[17] The principle of transparency establishes that the controller is obliged to take "any appropriate measure" to keep the data subjects informed about how their data are being processed.[18] This includes, for example, that the data subjects must be informed under Article 13 GDPR or Article 14 GDPR once their data has been obtained. Therefore, individuals, whose data is being processed for the purposes of fighting COVID-19 should receive **transparent information on the processing activities that are being carried out, including the retention period for collected data, the purposes of the processing and any likely transfer to third parties**. The information provided should be **easily accessible and provided in clear and plain language**, as also required in Articles 12-14 GDPR.[19]

Any processing of personal data must be done for a **specific, well-defined purpose** and personal data must then only be processed for additional purposes which are compatible with the original purpose (**purpose limitation**). Personal data collected for specific purposes, like monitoring the citizens´ compliance with governmental measures, conducting research or tracking of interactions with infected persons shall only be processed for these specified purposes. The purpose must be in line with the legal basis chosen by the controller or defined by national legislation and defined before processing has started. Processing of personal data for purposes different from the original one should comply with the requirements in Article 6(4) GDPR.[20] Further processing for scientific purposes is deemed to be a compatible new purpose.[21]

14 CJEU, C-342-12, *Worten*, May 2013, ECLI:EU:C:2013:355, pp. 24-43; CJEU, C-131/12, *Google Spain*, ECLI:EU:C:2014:317, pp. 70-75.
15 Example Council of Europe Modernised Convention 108, Art. 5 (2) and applicable national laws.
16 European Union Fundamental Rights Agency, "Handbook on European data protection law," 2018, p. 119, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.
17 Ibid p. 118.
18 European Union Fundamental Rights Agency, "Handbook on European data protection law," 2018, p. 120, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.
19 Ibid p. 119; see also Article 29 Working Party, "Guidelines on Transparency under Regulation 2016/679", WP 260, 2017.
20 See also Recital 50 GDPR.
21 Article 5 (1) (b) GDPR.

Data processing must be limited to what is really necessary to fulfil the chosen purpose in the fight against the virus (**data minimisation**). **As has been underlined by AccessNow, "a pandemic is no excuse to process extensive and unnecessary data".**[22] Personal data must be **accurate** and, where necessary, kept up to date. In cases where personal consequences may rely on data (e.g. limitation of movement, access to health care or saving people from infections) the accuracy of personal data is of great importance.[23] Furthermore, the **potential impact of an app is determined by the quality of data that the app collects**.

Once the purposes for processing are fulfilled, the data should be **deleted or anonymised (storage limitation)**. It has be suggested that, for example, when processing data about infected persons to monitor their condition or to check whether they respect the quarantine, the currently established timelines (e.g. the now common 14 days of quarantine from the infection) may form the basis for any storage limitation.[24] Following this period, if the data are further used for statistics or **scientific research purposes**, then the data should be anonymised, if identifiable information is not strictly needed for the given research purpose.[25]
Furthermore, personal data shall be processed in a manner that ensures appropriate **security. This includes** ensuring protection against unauthorised or unlawful processing and accidental loss, destruction or damage (**integrity and confidentiality**). For this purpose, appropriate technical or organisational measures must be implemented (Article 32 GDPR). Access to health data shall be limited to those who need the information for example to conduct treatment or research.[26] Taking security measures seriously is especially important when processing operations are conducted with short timelines and under pressure – as they are likely to be in the current state of emergency. Moreover, in the current emergency, many processing operations will relate to sensitive data concerning health. Given the sensitivity of this form of personal data special precautions must be observed. For example, data protection impact assessments under Article 35 GDPR are obligatory for all, processing involving the large scale processing of special categories of personal data (Article 35(3)(b) GDPR) or the systematic large scale monitoring of publicly accessible areas (Article 35(3)(c) GDPR).[27]

Finally, the last general data protection principle is the **accountability** of the controller. The principle states that the controller shall be responsible for, and be able to demonstrate compliance with, principles stated in Article 5 GDPR. Accountability also requires controllers and processors to actively and continuously implement measures to promote and safeguard data protection in their processing activities.

A situation of emergency like the COVID-19 pandemic will often allow processing under different

22 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 7, available at: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.
23 See GDPR Hub, "Data Protection under SARS-CoV-2," available at https://gdprhub.eu/index.php?title=Data_Protection_under_SARS-CoV-2.
24 Ibid.
25 Ibid.
26 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 7, available at: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.
27 See GDPR Hub, "Data Protection under SARS-CoV-2," available at https://gdprhub.eu/index.php?title=Data_Protection_under_SARS-CoV-2.

legal basis; the data protection principles here listed are, therefore, paramount in containing disproportionate processing. In this regard, **the least intrusive solution, in light of the purpose to be achieved, is always to be preferred**. This implies that, for example, **if the purpose pursued by the app could be achieved without personally identifiable information, this option should be pursued**. In this way in particular the principle of data minimisation would be complied with.[28] As the EDPB has noted, "invasive measures, such as the "tracking" of individuals (e.g. processing of historical non-anonymised location data) may be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing".[29] Further, "however, it should be subject to **enhanced scrutiny and safeguards** to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation)".[30] The concept of "privacy by design and by default" (Article 25 GDPR) is therefore crucial in the design process for tracking applications.

5. DATA SUBJECTS RIGHTS

The EU data protection framework confers several rights on data subjects. These rights (listed in Articles 12 to 23 GDPR) include, amongst others, **rights to information, access, rectification, data portability**. These rights are highly relevant to any COVID-19 related processing. **App providers therefore need to provide proper information about the applicability of data subject rights**. Information about data subject rights shall be included in the privacy policy. In practice, app developers should ensure that the **app architecture facilitates the exercise of data subject rights**. For example, the app should be designed to facilitate the right to access.

28 CJEU C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, 11 December 2019, ECLI:EU:C:2019:1064, p. 48-51.

29 European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020, p. 3, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf; Italian DPA, "Interview with Antonello Soro", available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9294705.

30 European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf; Italian DPA, "Interview with Antonello Soro", available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9294705.

II. EXAMPLES COVID-19 TRACKING APPS

Following the example of East Asian countries such as South Korea, China and Taiwan, several apps have been developed in different EU Member States to track citizens as a response to the COVID-19 pandemic.[31] In the following, we provide a short list of the types of application which currently exist.[32]

Types of application:

- **Contact tracing app:** apps which track infected people and alert other people who have been exposed, once a person is COVID-19 positive
- **Enforcement of lock-down:** apps which monitor citizens in quarantine
- **Scientific purposes, risk map and statistical analysis:** apps which processes location information
- **Self-assessment app:** apps which facilitates self-testing by citizens and tracking of the disease by health professionals

An overview of the main data protection issues related to a selection of specific apps is provided in the table below and in the brief analysis following the table.

1. COVID-19 TRACKER APPS – TABLE 1

GDPR requirements	PEPP-PT (EU-wide)[33] – contact tracing app	Stopp-Corona-APP (AT)[34] – contact tracing app	CORONAMADRID (Spain)[35] – self-assessment app
Purpose	To measure proximity, track and stop the spread of COVID-19	To stop the spread of COVID-19 by contact tracing	To help citizens self-assess the probability of suffering from COVID-19
Anonymised[36]	Yes, as claimed by developers	Pseudonymised	As claimed by developers
Data minimization	Yes, as claimed by developers	Yes – phone number and whether tested positive for COVID-19 (health data)	As claimed by developers
Consent (in the data protection field?)	Not clear whether consent fulfils requirements of GDPR and ePrivacy	Not clear whether consent fulfils requirements of GDPR and ePrivacy	Not clear whether consent fulfils requirements of GDPR and ePrivacy
Voluntary participation	Yes	Yes	Yes
Deletion period (of the data or the whole app?)	Data is not stored on the app or anywhere else, as claimed by developers	30 days for infected persons; for non-infected – as long as they use the app; contact data – after the end of the epidemic; for purposes of prosecuting illegal usage – 3 years after the end of the sickness;	"as long as the health emergency lasts"
Encryption	Yes, as claimed by developers	Yes	Yes
Geolocation data/GPS	No	No	Yes (optional)

31 Nicholas Wright, "Coronavirus and the Future of Surveillance: Democracies Must Offer an Alternative to Authoritarian Solutions," Foreign Affairs, April 2020, available at https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance.

32 See GDPR Hub, "Data Protection under SARS-CoV-2," available at https://gdprhub.eu/index.php?title=Data_Protection_under_SARS-CoV-2.

33 Janosch Delcker and Stephen Brown, "Europe shares code for new coronavirus warning app," Politico, April 2020, available at https://www.politico.eu/article/europe-cracks-code-for-coronavirus-warning-app/; Pan-European Privacy-Preserving Proximity Tracing, available at https://www.pepp-pt.org/; Fraunhofer IUK-Technologie, "PEPP-PT: Pan-European Privacy-Preserving Proximity Tracing: Kontakterfassungs-Framework zur Bekämpfung der Ausbreitung von Covid-19," available at https://www.iuk.fraunhofer.de/de/themen/loesungen-und-kompetenzen-zur-bewaeltigung-der-corona-krise/pepp-pt.html; Fraunhofer AISEC, "Pressemitteilung: Fraunhofer AISEC erarbeitet Sicherheitskonzept Privacy Protecting Proximity Tracing: Multinationale Initiative entwickelt digitale Lösung im Kampf gegen Corona," April 2020, available at https://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/presse/pressemitteilungen/2020/PEPP-PT.html.

34 Österreichisches Rotes Kreuz, "STOPP CORONA – MEIN KONTAKT-TAGEBUCH," available at https://www.roteskreuz.at/site/faq-app-stopp-corona/; and the data protection information notice is available at https://www.roteskreuz.at/fileadmin/user_upload/Stopp_Corona_App_DatenschutzInformation__OeRK_24.03.2020_V1.1.pdf.

35 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 21, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.

36 Please see para III 2. It is questionable, whether it is feasible to effectively anonymise app data. For further important criticism with regard to this app, see: PEPP-PT_ Data Protection Architechture - Security and privacy analysis available at: https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf.

2. COVID-19 TRACKER APPS – TABLE 2

GDPR requirements	"Stay- healthy"[37] app (Slovakia) contact tracing app	AllertaLOM (Italy, Lombardia) – risk map and statistical analysis	"Home quarantine" (Poland)[38] – quarantine enforcement	Germany, RKI app (DE)[39] scientific purposes and risk map
Purpose	To inform the user if someone infected with COVID-19 is in close proximity	To track the spread of COVID-19 in the region; to create a contagion risk map; to conduct statistical and epidemiological analyses	To confirm the location of a person covered by the quarantine restrictions and to conduct basic health assessment	Research purpose: to help RKI understand and map better the spread of COVID-19
Anonymised[40]	Yes according to sources – user registers with phone number or email address but receives a unique registration number	Not clear	Not clear	Pseudonymised
Data minimization	Not known	As claimed by developers	No	Collects data from wearables (of other providers) and main body indicators + ZIP code; allows profiling
Consent (in the data protection field?)	Not clear	Not clear whether consent fulfils requirements of the GDPR and ePrivacy	Not clear whether consent fulfils requirements of GDPR and ePrivacy	Yes
Voluntary participation	Yes	As claimed by developers and controllers	It seems to be mandatory	Yes
Deletion period (of the data or the whole app?)	Not known	"for the time strictly necessary to study the degree of spread of the infection"	"as long as the health emergency lasts"	Not known
Encryption	Not known	Yes	Not clear	Yes
Geolocation data/GPS	According to the sources, users are not tracked.	Yes	Yes	Zip-code

37 Ibid pp. 18-19; Stanislav Vinc, "Appka Zostaň zdravý upozorní na koronavírus v okolí," Techbox, March 2020, available at https://techbox.dennikn.sk/aplikacia-zostan-zdravy-vas-upozorni-na-potvrdenie-koronavirusu-vo-vasom-okoli/; "The Slovak app alerts you if you are near a person infected with coronavirus," EngNews24h, March 2020, available at https://engnews24h.com/the-slovak-app-alerts-you-if-you-are-near-a-person-infected-with-coronavirus-communication-science-and-technology/.

38 Ibid; Privacy International, "Poland: App helps police monitor home quarantine", March 2020, available at https://privacyinternational.org/examples/3473/poland-app-helps-police-monitor-home-quarantinee.

39 RKI, Corona-Datenspende faq, available at https://corona-datenspende.de/faq/.

40 Please see para III 2. It is questionable, whether it is feasible to effectively anonymise app data.

III. MAIN DATA PROTECTION REQUIREMENTS TO BE TAKEN INTO CONSIDERATION

1. VOLUNTARY USAGE OF THE APPS AND CONSENT

In the current situation, people may be subject to significant psychological and peer pressure to download an app and provide the necessary information. Therefore, in cases where consent is used either as a legal basis for downloading the app or for providing certain personal data via the app, care should be taken when evaluating the applicability of consent as a legal basis, in particular as to whether, under current circumstances, **consent can truly be considered to be "freely given"** – one of the core requirements of consent in data protection law.[41]

2. ANONYMOUS VS PSEUDONYMOUS DATA

In the context of COVID-19, certain applications seem to rely on **location tracking** to map the evolution of the virus and **monitor the behaviour of citizens** (e.g. in the case of apps such as "AllertaLOM", "Home quarantine" or "Stopp Corona"). Such tracking comes with several concerns. Location data is highly revealing; home address, workplace, social interactions, habits and so on can be deduced by simply following a person's movement.[42] Such highly revealing information comes in addition to the collection and further processing of large quantities of health data. Thus, **the potential to derive information about the app users from combining these different types of information is significant**. Hence, the data protection safeguards need to be strictly complied with.

Furthermore, even if location tracking apps were to try to anonymise personal data – e.g. as asserted by the developers of PEPP-PT – some scientists argue that **anonymous location data can be easily re-identified**. Indeed, "an individual's identity can easily be deduced from just a handful of anonymized mobile phone location data points."[43] In this regard, **it may not be feasible to effectively anonymise app data**. As the CJEU has established, data could fall under the definition of "personal data" even if the pieces of information allowing the unique identification of an individual are not in the hands of one entity, as long as there are legal means for one entity to have access to the different pieces of identifiable information leading to the identification of an individual.[44] Accordingly, controllers have to make sure no actor has the ability to re-identify the data with means that "account should be taken of all the means *likely reasonably to be used* (...) to identify the said person".[45]

In consequence, **data are, from a legal perspective, potentially pseudonymous rather than anonymous**, even if they are described as ano-

41 Article 7 GDPR and Recital 32 GDPR and Article 5 (3) ePrivacy Directive. See also Article 29 Working Party, "Guidelines on Consent under Regulation 2016/679," 10 April 2018.

42 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 9, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.

43 Kim Zetter, "Anonymized Phone Location Data Not So Anonymous, Researchers Find", Wired, March 2013, available at https://www.wired.com/2013/03/anonymous-phone-location-data/; see also: Vincent Manancourt, Janosch Delcker, Mark Scott and Laurens Cerulus, "In fight against coronavirus, governments embrace surveillance", Politico, March 2020, available at https://www.politico.eu/article/coroanvirus-covid19-surveillance-data/.

44 CJEU, C-582/14, *Breyer*, 19 October 2016, ECLI:EU:C:2016:779, par. 40-49.

45 Ibid, par. 42.

nymous by developers and operators. Pseudonymous data, in contrast to anonymous data, fall within the scope of the GDPR.[46]

3. DATA ACCURACY

The use of location data to determine whether people have been in contact with someone infected by the virus (as in the "Stopp Corona" contact tracing app) has been argued to have **significant technical limitations.**[47] Cell tower location tracking, for example, cannot detect whether two phones were within two meters of each other (which could be relevant information in the case of monitoring contact with infected people); GPS signals could offer better precision but still suffer of several limitations (e.g. these do not work properly inside buildings or in vehicles).[48] This is a data accuracy problem, which could hinder the app from achieving its declared purpose, which begs the question whether the data processed by such apps are appropriately accurate.[49]

Another **data accuracy problem** is that the app might continue tracing individuals after they have ended their quarantine period, e.g. as was reported in the case of Poland. Pursuant to a news article, individuals were subject to disproportionate interference by the authorities because of inaccurate information. For example, a person whose quarantine period had ended was asked to verify that he was at home, even though he was allowed to go out.[50]

Furthermore, with regards to the **quality of data the apps collect**, in the case of a contact tracing app like the "Stopp Corona", data quality will depend, for example, on the "traceability of users", and on the "availability, state, and usage of the mobile device".[51] As scientists of KU Leuven describe, "mobile phone-based solutions for contact tracing rely on two fundamental yet questionable, assumptions." They clarify that "the proximity of two mobile phones is deemed a proxy for virus transmission. Virus transmission, however, does not depend only on proximity; it depends mainly on the nature of the interaction (...) and also on the infectiousness of the infected person, the stage of the disease, etc."[52] Further, "a mobile phone is deemed as a proxy for a person. The person-phone relationship or correlation, however, is shaped by values and practices."[53] For example, some people keep the device near their body, others keep the phone distant from them.[54] In the case of a self-assessment app like CORONAMADRID, which require data input from participants, numerous other factors can affect data quality, for example participants may forget to enter the data, or they may be subject to recall bias, self-reporting might not be done properly or it may be highly subject to response bias (e.g. when users fear potential stigma).[55]

These examples demonstrate that the principle of data accuracy, as enshrined in Article 5 (1) (d) GDPR, is not always complied with. As explained

46 Recital 26 GDPR.
47 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 13, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.
48 Ibid. pp. 13-14.
49 CJEU, C-293/12 and C-594/12, *Digital Rights Ireland*, April 2014, ECLI:EU:C:2014:238, par. 49.
50 Mark Scott and Zosia Wanat, "Poland's coronavirus app offers playbook for other governments", Politico, March 2020, available at https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/.
51 KULeuven, "Contact Tracing Tools for Pandemics: factors that should shape the decision-making to deploy contact tracing apps for pandemic containment measures", available at https://rega.kuleuven.be/if/tracing-tools-for-pandemics.
52 Ibid.
53 Ibid.
54 Ibid.
55 Ibid.

at the beginning, compliance with the data protection principles is one of the requirements on legality of personal data processing.

4. TRANSPARENCY

Transparency[56] about how data flows between public and private entities involved in the development and operation of the apps should be given special consideration. Opaque deals with telecoms operators and companies to share e.g. location data, pose serious risks to people's privacy.[57] Therefore, as has been recommended by AccessNow, "**telecoms operators and companies processing data should work with supervisory authorities and privacy experts to ensure data appropriate safeguards**.[58] As AccessNow states, "private-sector actors that design, develop, or implement systems to tackle COVID-19 should follow an industry standard **human rights due diligence framework** to identify salient risks, avoid fostering discrimination, and respect human rights more broadly through all lifecycles of their systems".[59] Further, "as necessary, private sector actors should create processes to monitor, mitigate, and report on potential harms and notify affected individuals."[60] The public sector must provide data protection impact assessments. These assessments should be continually revisited – "prior to public procurement, during development, at regular milestones, and throughout their context-specific use".[61] The assessments must be made available to the public in an easily accessible format".[62] Governments should consider "the human rights track record" of companies and refrain from using apps from actors that that infringe human rights on a systematic basis.[63] Furthermore, **data management principles and practices** (e.g. where the data is stored and for how long, how secure is the system, who has access, is the data anonymized) **must be well planned and transparent**.

5. RE-USE OF DATA COLLECTED BY APPS

When relying on private companies, there is a strong risk associated with **monetisation of health information**. There should be **clear limitations on the secondary uses of data** so that the principle of purpose limitation is complied with.[64] It could be the case that health data is sold or transferred to third parties who are not working in the public interest. This practice might be included in the privacy policies in the apps, to which app users give their consent. However, even if app users consent to such a re-usage of their data, in so far as consenting to this re-usage would be voluntary and based on clear and unambiguous information about the re-usage, and thus such processing would have formally a legal basis, there might be still ethical and moral problems about this re-usage.

As noted by Privacy International, "data can be essential and useful at various stages of a pandemic and public health emergency. However, it can also feed **intelligence and policing**, being highly useful for **enforcement**"[65] (the "Home quarantine"

56 Article 5 (1) (a) GDPR.
57 AccessNow, "Recommendations on privacy and data protection in the fight against COVID-19," March 2020, p. 21, available at https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf.
58 Ibid.
59 Ibid, p. 21.
60 Ibid.
61 Ibid.
62 Ibid.
63 Ibid, p. 22.
64 Article 5 (1) (b) GDPR.
65 Privacy International, "Covid-19 response: overview of data and technology", March 2020, https://privacyinternational.org/key-resources/3547/covid-19-response-overview-data-and-technology.

app is an example of this).[66] This is especially the case if the legitimate purposes of the app are not clearly specified or if they are broadly phrased to allow law enforcement authorities such as the police – e.g. as in Poland – to have access to the data processed by the app. There is a risk that the app might be used for purposes beyond enforcing quarantine or monitoring the spread of the virus. Finally, **re-use of personal data for scientific and research purposes is considered to be a compatible re-use of data provided this complies with Article 89 GDPR and with other data protection principles.**[67] If data is to be shared at a later stage (after the emergency) for research purposes (e.g. as claimed by AllertaLOM), however, in order to comply with the data minimisation principle and Article 89 GDPR, apps should be clear as to what level of granularity of data researchers need to receive.[68] Consequently, **where, for the research in question, only anonymous data is necessary, all steps should be taken to make sure that researchers only receive anonymous data.**

6. CENTRALISED VS DECENTRALIZED STORAGE

An important data protection question concerning **the possibility of (incompatible) data re-use** is where the data collected by the app are stored, i.e. whether only locally on a user's device (e.g. as claimed by PEPP-PT) or whether there is a central collection of data, e.g. as in Slovakia or the case of the RKI app. The latter scenario may allow governmental authorities much easier access to the data and the subsequent processing thereof, both for purposes compatible with the original purpose of the processing, but also for incompatible purposes. Thus, **the local storage scenario is the more data protection friendly choice.**

A related problem with centralized storage is that the data subject (app user) has less control over the processing of their data and has less control over the parties to whom data is disclosed, for which purposes, etc. There is a risk that the subject also cannot easily verify the accuracy of the data processed by the app and the profile made in relation to them if the data are not stored and further analysed on the app but are instead stored on a central database. For example, according to the information provided in relation to the RKI app, the data are transmitted, stored and analysed in a data centre and the analysis of the data seems not be accessible to the app users.

7. SUNSET CLAUSE FOR THE APPS

Experience has taught us that there is a high risk governments may not lift exceptional **surveillance measures** after the event leading to the measures is over.[69] Some apps promise users that data will be deleted after the COVID-19 emergency (e.g. CORONAMADRID). However, since this period is not determined and the emergency measures could be in place for a long time, it is not clear why all the data collected via the app need to be stored until the emergency is over and may not be deleted before. In the case of the

66 In China, for example, data from the app have been apparently automatically transferred to the police, see: Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," The New York Times, March 2020, available at https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

67 Article 5 (1) (b) GDPR.

68 KULeuven, "Contact Tracing Tools for Pandemics: factors that should shape the decision-making to deploy contact tracing apps for pandemic containment measures", available at https://rega.kuleuven.be/if/tracing-tools-for-pandemics.

69 Colin J. Bennett and Kevin Haggerty, "Security Games: Surveillance and Control at Mega-Events," April 2011, Routledge; Arne Wiechern and Peter Schaar, "Schutz vor Corona oder Schutz der persönlichen Daten: Was wiegt mehr?", SWR, available at https://www.swr.de/swraktuell/radio/im-gespraech/schutz-vor-corona-oder-schutz-der-persoenlichen-daten-was-wiegt-mehr-100.html.

Polish "Home Quarantine" app, all the data collected (e.g. selfies/digital photos and GPS location data) will be kept for 6 years. However, this **duration of COVID-19 health data storage has to be legally justified, i.e. the storage of the data needs to be proportionate.**[70] Yet, it is not clear why, if the emergency were to be over before 2026, the data would still need to be stored until this date. This is likely to be in conflict with the requirement on limited data storage (Article 5 (1) (e) GDPR). As regards "sunset" clauses, the **apps should be designed in such a way as to "delete" themselves (or have a delete button)** and stop operating once the pandemic is over and to make sure that current surveillance measures, enabled by the apps, are lifted after the pandemics is over.

8. DATA SECURITY AND INTERNATIONAL DATA TRANSFERS

As apps may have been built quickly, given the speed with which the emergency situation arose, **security** protections may suffer as developers may not have enough time to check for bugs or technical flaws (e.g. "Home Quarantine").[71] For instance, the risk of **hacking** when Bluetooth is used to track people's movements is especially high.[72] In addition, it is not always the case that data are stored in the EU, e.g. in the case of Stopp-Corona, data could be transferred to the USA. This could pose an additional security and data protection challenge. In that respect, there is also a risk that the data are accessed by foreign authorities for purposes not related to the fighting of the virus in the respective EU Member State where the app is operational. In addition, as the EDPS has noted, even if no personal data is processed, the information security requirements stemming from Commission Decision 2017/46 still apply.[73] For example, the guidelines concerning security requirements in relation to digital health applications, issued by the German Federal Office for Information Security (BSI), could provide useful guidance to app developers, e.g. on how to ensure the confidentiality, integrity and availability of the data processed by these apps.[74]

9. DATA SUBJECT RIGHTS

Last but not least, EU data protection law foresees a series of data subject rights – the right to information, access to one's own personal data, to rectification and erasure of one's data, the right to restriction of the processing of one's data, the right to object to the processing of one's data, the right to data portability and the right not to be subject to a decision based solely on automated processing.[75] The controllers of the apps should **enable the exercise of these rights. Restrictions** to the above-mentioned rights are possible, however, they **must be based in law and must respect the essence of the fundamental rights and freedoms and be necessary and proportionate in a democratic society.**[76] For example, in the EU, it is not legal that automated decisions are to be taken on whether people are allowed to go out or not or whether a person might be contagious or not, unless these fulfil the criteria in Article 22 GDPR.[77]

70 Mark Scott and Zosia Wanat, "Poland's coronavirus app offers playbook for other governments", Politico, March 2020, available at https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/; Digital Rights Ireland, par. 63-64.
71 Mark Scott and Zosia Wanat, "Poland's coronavirus app offers playbook for other governments", Politico, March 2020, available at https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/.
72 Clemens Haug, "Handy-App statt Ausgangsbeschränkung?", Mdr Wissen, available at https://www.mdr.de/wissen/corona-epidemiologie-ausbreitung-virus-handy-app-100.html.
73 European Data Protection Supervisor, "Monitoring spread of COVID-19", March 2020, available at https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.
74 Bundesamt für Sicherheit in der Informationstechnik, "BSI TR-03161 Sicherheitsanforderungen an digitale Gesundheitsanwendungen", 2020.
75 Chapter III GDPR.
76 Article 23 GDPR.
77 Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," The New York Times, March 2020, available at https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

10. CURRENT PROPOSALS ON APPS WHICH ARE PRIVATE BY DESIGN

Recently, a group of well-known academics proposed a **decentralized privacy-preserving proximity tracing system** – a system designed such that no entity beyond a user's device processes or stores any personal data. They assert that this system "minimises the amount of personal data collected by one entity, and heavily reduces the possibility of the accessibility of information, providing the guarantee that the backend server learns nothing about identifiable individuals or their health status".[78] Consequently, the server cannot have knowledge about the social graph (data that can easily be repurposed and misused) and function creep may be prevented.[79] Furthermore, "(a)ll ll communications between the app and the backend server, or any other party, are encrypted using the most appropriate TLS configuration".[80] The system ensures data minimization: the central server only observes anonymous identifiers of infected people without any proximity information; health authorities learn no information (beyond when a user manually reaches out to them after being notified) and the epidemiologists obtain an anonymized proximity graph with minimal information.[81] Moreover, the scientists argue that it prevents abuse of data "as the different entities in the system receive the minimum amount of information tailored to their requirements"[82] and further prevents tracking of non-infected users.[83] In addition,"(t)he system will organically dismantle itself after the end of the epidemic."[84] Further, "infected patients will stop uploading their data to the central server, and people will stop using the app. Data on the server is removed after 14 days".[85] The system envisioned could provide a virtuous example useful for other apps.

78 Decentralized Privacy-Preserving Proximity Tracing, Overview of Data Protection and Security, p. 4, available at https://github.com/DP-3T/documents.
79 Ibid p. 4.
80 Ibid p. 6.
81 Decentralized Privacy-Preserving Proximity Tracing, White Paper, p. 2, available at https://github.com/DP-3T/documents.
82 Ibid.
83 Ibid.
84 Ibid.
85 Ibid p. 2 and 3.

IV. RECOMMENDATIONS

The analysis in the previous sections revealed a number of risks which tracing apps could pose for privacy and data protection. In order to mitigate these risks, **developers and controllers** of these apps should implement at least the following recommendations:

- Apps should be **private and secure by design**. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data[86] to protect these against unauthorised processing or accidental loss. For this purpose, **appropriate technical or organisational measures** must be implemented as laid down in Article 32 GDPR. For COVID-19 tracing apps, a decentralized tracing system (see para III 10) is highly recommended. Data should be rather stored **locally on the users device instead of centrally collected**.
- **Access to personal, especially sensitive, data** shall be limited to those who need information to conduct treatment, research, and otherwise address the crisis. The information should be stored and transferred securely, e.g. through **robust encryption measures** (security).
- The app should be designed in such a way as to **automatically dismantle itself (or have a delete button)** and stop operating once the pandemic is over to make sure that the current surveillance measures, enabled by the app, do not last longer than necessary for responding to the pandemic **(sunset clause)**.[87]
- Once the purpose of processing is fulfilled, the data must be **deleted or anonymised**. For example, when processing data about infected persons, e.g. to monitor compliance with quarantine restrictions, the currently established timelines, i.e. the now common 14 days of quarantine from the time of infection or the necessity to go into quarantine (for those coming back from an affected area), should form the basis for any storage limitation.
- If the purpose pursued by the app could be achieved **without personally identifiable information**, this option should be pursued.
- Controllers should **minimize the re-identification risks and make sure no actor has the ability to re-identify the data**.
- The data flow between public and private entities collaborating in deploying an application should always be **transparent**,[88] as should the processing of the personal data, the retention period, the purposes of the processing, any likely transfer to third parties and the rights of the data subjects.

86 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," 21 April 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, p.9. "European Commission, "Commission Recommendation of 8.4.2020 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," 08 April 2020, C(2020) 2296 final, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, p. 10.

87 European Commission, "Commission Recommendation of 8.4.2020 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," 08 April 2020, C(2020) 2296 final, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, p. 10. 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," 21 April 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, p. 8.

88 European Commission, "Commission Recommendation of 8.4.2020 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," 08 April 2020, C(2020) 2296 final, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, p. 10.

- Controllers and developers **need to provide proper information about the applicability of data subject rights** and should ensure that the **app architecture facilitates the exercise of data subject rights**.
- Controllers and developers **should work with supervisory authorities and privacy experts to ensure data appropriate safeguards**.
- The apps **must have clear limitations on the secondary uses of data and re-use of personal data for scientific and research purposes must comply with Article 89 GDPR** and other data protection principles. For example, **wherever possible, data should be anonymized, where possible, when further used for statistics or research purposes** (storage limitation).
- Developers and controllers should carry out a **data protection impact assessment (DPIA),**[89] especially where the apps could collect or derive sensitive data or permanently track individuals. This should to be made available to the public in an easily accessible format and be updated regularly.
- The processing of the data via the apps should ensure the processing of **accurate input data and results.**[90] In addition, the app users should always have the opportunity to refute the information and to have it corrected, e.g. so that they are not banned from leaving their homes after the quarantine is over.
- **Derogations** from the data protection principles and the rights of the data subject should comply with Articles 23 and 89 GDPR and Article 15 ePrivacy Directive.
- To prevent abuse, apps should clearly regulate who may have access to the data processed on a **need-to-know basis.** The purposes of access and further processing should be clearly stated and restricted.

89 Article 35 GDPR. 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," 21 April 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, p. 8 and 9.

90 Article 5 (1) (d) GDPR.