cepAdhoc

No 4 | 2020 21 April 2020

Contact tracing apps under EU personal data protection law

"Freely given" consent of individuals is a prerequisite for the next step in the fight against COVID-19

Martina Anzini

Contact tracing apps are expected to play an important role in the fight against the Coronavirus. The EU privacy and personal data protection framework, however, establishes legal constrains on such apps.

- Proximity recording apps – that only record epidemiologically relevant contacts – are a more personal data protection-friendly alternative to location data recording apps. For this very reason, the legitimacy of the latter can be ruled out.
- Proximity recording apps can operate without personal data, thus making the related data processing fall out of the scope of the General Data Protection Regulation (GDPR).
- The E-Privacy Directive, however, applies. It establishes a general prohibition for apps to store information on smartphones and to access information already stored on smartphones. This prohibition can be overcome through consent. Therefore, contact tracing apps can only lawfully operate with the consent of users.
- This consent must be "freely given". Therefore it cannot be obtained by Member States by making the right to the movement of persons conditional upon the use of the app.
- Member States are not allowed to legally impose the use of a proximity recording app either, because they lack the legal ground to derogate from the above prohibition pursuant to the E-Privacy Directive.

Table of Content

1 Digital contact tracing

The World Health Organisation (WHO) defines contact tracing as a monitoring process that involves identifying and managing the contacts of probable or confirmed cases of infection. This enables the health authorities (i) to swiftly treat the persons infected by a contagious disease and (ii) to rapidly identify secondary cases that may arise after transmission from the primary known cases, with the aim of interrupting further transmission. Contact tracing is carried out by means of the following steps:

1. identifying the contacts of the person who has been found to be infected;
2. informing such contacts about (i) their contact status, (ii) what the contact status means for them, (iii) the actions that they are supposed to undertake as potentially infected persons and (iv) the importance of receiving early care if they develop symptoms; quarantine or isolation could be required for high risk contacts;
3. a regular follow-up of contacts to monitor for symptoms and test for signs of infection.[1]

According to the European Centre for Disease Prevention and Control (ECDC), "[c]ontact tracing is an essential measure to fight the ongoing epidemic of COVID-19, in conjunction with active case finding and testing, and in synergy with other measures such as physical distancing".[2] The ECDC reports that this evaluation is based, inter alia, on emerging evidence regarding the evolution of the pandemic in China and Singapore. In those countries, efficient contact tracing minimised the time lapse between onset of symptoms and isolation and is believed to have greatly contributed to an effective fight against the virus.[3]

The most traditional form of contact tracing involves asking the infected person about his movements and the persons he was in contact with within the relevant timeframe ("the contacts"). Digital technology, however, enables health authorities to use alternative and more efficient strategies – i.e. strategies that minimise the costs of contact tracing in terms of time and the demand on human resources. In this regard, the following options are available:

- record of location data to rapidly track the places the infected person visited within the relevant timeframe and check the persons who also visited those places at the same time; or
- record only of epidemiologically relevant events of proximity of the infected person to other persons, so that the latter can be swiftly identified.

Whatever the selected option, smartphone apps seem to be the best tool to implement it, given that (i) a large part of the population owns a smartphone, (ii) people carry them continuously and (iii) users exercise exclusive control over them (meaning that people do not generally "lend" smartphones to others).[4]

---

1 https://www.who.int/features/qa/contact-tracing/en/

2 ECDC, Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, p. 2.

3 ECDC, Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, p. 2.

4 Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, p. 7.

Both options raise, at least potentially, issues of compatibility with the EU privacy and personal data protection framework. While their final configuration will have a huge bearing on the very existence and nature of data protection concerns, it seems relevant to explore the applicable personal data protection law. This will be the object of this paper.

2 Digital contact tracing options under EU data protection law

2.1 Relevant personal data protection instruments under EU law

The legality of digital contact tracing, as far as data processing and restrictions of privacy are concerned, must be assessed in reference to the General Data Protection Regulation (GDPR) and the E-Privacy Directive.

- The GDPR[5] lays down rules concerning (i) the protection of natural persons with regard to the processing of personal data and (ii) the free movement of such data across the internal market.[6]
- The E-Privacy Directive[7,8] (i) harmonises the national provisions that protect the right to privacy and confidentiality with respect to personal data processing in the electronic communication sector and (ii) ensures the free movement of such data and of electronic communication equipment and services across the EU.[9] Its stated aim is to particularise and complement the GDPR[10] for the purposes of personal data protection and the free flow of personal data in the telecoms sector.[11]

2.2 Option I - A location data recording app

Smartphones allow for constant monitoring of location data by relying on different technological infrastructures. Among them, notably, the Global Positioning System (GPS), GSM base stations and WiFi.[12]

A contact tracing app could record and store all location data of all app users to enable tracking the movements of each individual. If a subject proves to be infected, all app users who have been in contact with him will be spotted by crossing their location data with those of the COVID-19 case. They will consequently receive a warning message.

Location data is protected by the GDPR because it qualifies as “personal data”. Indeed, any pro-

5 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), OJ L 119, 4.5.2016, p. 1.

6 Article 1 (1) GDPR.

7 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.

8 On the Proposal COM(2017) 10 of 10.01.2017 for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communicationsand repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), see Eckhardt P. and Hoffman A., https://www.cep.eu/en/eu-topics/details/cep/privacy-and-electronic-communications-regulation.html .

9 Article 1 (1) Directive 2002/58/EC.

10 References to the old Personal Data Protection Directive (Directive 95/46/CE) in the E-Privacy Directive must be now understood as references to the GDPR (see Article 94 para. 2 GDPR).

11 Article 1 (2) Directive 2002/58/EC.

12 See Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011.

cessing of information relating to an identified or an identifiable natural person falls under the GDPR.[13] Furthermore, processing of location data - i.e. data processed in an electronic communications network or by an electronic communication service, indicating the geographic position of the terminal equipment of the user - is subject to strict limitations under the E-Privacy Directive.[14]

In a document recently addressed to the Commission, the European Data Protection Board (EDPB) voiced criticism about a location data recording app. Notably, according to the EDPB, location data processing is not strictly necessary to achieve the purpose of effective contact tracing because a different and less intrusive option exists, i.e. proximity recording.[15] This has led the EDPB to conclude that, besides creating security and privacy risks, "[c]ollecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation".[16,17] In its recent Guidance, the EU Commission has upheld the position of the EBPB.[18]

2.3 Option II - A proximity recording app

The alternative to a data localisation recording app is an app that only records and stores epidemiologically relevant contacts. According to the Commission, the app should rely on Bluetooth technology and could work as follows. [19]

1. The app will generate temporary identifiers of the smartphone[20] and collect via Bluetooth the temporary identifiers which are produced by the apps operating in nearby devices.

2. Such detections ("handshakes") will be recorded in a decentralised fashion on the phone or centrally on a server[21] only when the contact is epidemiologically relevant, i.e. when it entails an actual risk of infection.[22] This means that the contact needs to last long enough and be characterised by a sufficient level of physical proximity for the virus to be transmitted.

3. Finally, the warning mechanism that would alert app users that they have had an epidemiologically relevant contact with a COVID-19 case will differ depending upon whether the recording is centralised or not. In the former case, i.e. where the infected subject's contact history is uploaded onto a central database, app users with matching identifiers will be automatically notified that they may have been exposed (backend server solution). In the latter case, i.e. where the contact history is stored on the device, the app user found to be a

[13] Article 4(1) of the GDPR.
[14] Art 5(1), 6 and 9 E-Privacy Directive.
[15] "Contact tracing apps do not require location tracking of individuals users. Their goal is not to follow the movements of individuals or to enforce prescriptions" (https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf).
[16] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf
[17] The data minimisation principle, laid down in Article 5(1)(c) of the GDPR, provides that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".
[18] Communication from the Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, C(2020) 2523, Brussels, 16.4.2020 (Commission Guidance).
[19] Commission Guidance, p. 9.
[20] Consisting of sequences of numbers and letters that change over time.
[21] The decentralised solution is more in line with the minimisation principle. Health authorities should have access only to proximity data from the device of an infected person so that they are able to contact people at risk of infection (Commission Guidance, p. 10).
[22] Commission Guidance, p. 9.

COVID-19 case can send an alert to the other app users whose identifiers are listed in his contact history (decentralised processing).

2.3.1 The necessity of the consent of the app user

According the Commission, the temporary codes that the app generates and collects only enable the contacts to receive an alert on their smartphone.[23] They do not allow for identification of the smartphone or its owner. Thus, the above codes do not qualify as personal data and their processing falls outside the scope of application of the GDPR.[24]

Storing information on the user's device or gaining access to the information already stored is, however, still governed by the EU personal data protection framework, as Article 5 of the E-Privacy Directive applies. Pursuant to the Directive, those activities are only allowed:

- if intrinsically necessary to provide the information society service; or
- with the consent of the subscriber/user.

The Commission believes that part of the data that is required for the contact tracing exceeds what is strictly necessary to make the app work, e.g. the temporary codes of other users. The storage and accessing activities are, thus, not intrinsically necessary. Their lawfulness is, therefore, conditional upon consent of the user.[25]

According to the E-Privacy Directive, consent must be provided in a clear and comprehensive fashion with reference to, inter alia, the purpose of the processing. The concept is akin to that of consent under Article 6 (1)(a) GDPR.[26] This reference to the GDPR is particularly relevant because it prevents Member States from lawfully making the use of the contact tracing app a condition for enjoying the freedom of movement.

In fact, the interpretation of consent under Article 6 (1)(a) GDPR must be in line with the fundamental rights-oriented approach of personal data protection legislation. This means that, since the importance of the data subject's control over his data is expressly acknowledged by the current legal framework, the requirement must be construed so as to confer upon the data subject substantial – and not merely formal - control over his own data.[27] This approach to the interpretation of consent should also guide the understanding of the characteristics that consent must possess, under Article 4 (1)(11) GDPR, in order to be valid for data processing purposes. Under this provision "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she [...] signifies agreement to the processing of personal data relating to him or her".[28]

The requirement that consent be "freely given"[29] therefore means that the data subject must have a genuine choice between accepting and refusing. This would hardly be the case if the data subject

[23] "If the health authorities wish to contact the users who have been in close contact with an infected person also via phone or SMS, they need the consent of those users to provide their phone numbers" (Commission Guidance, p. 9).
[24] Considerandum 26 GDPR.
[25] Commission Guidance, p. 6.
[26] Article 5 (3) E-Privacy Directive.
[27] Article 29 Working Party (2017), p. 9.
[28] Article 4(11) GDPR.
[29] Article 4 (1) and (11) GDPR.

were given the option of either using the app or suffering severe restrictions of his freedom of movement. In other words, Member States cannot make the right of persons to move freely dependent upon them using the app. Such conditionality would mean that the consent given by persons has not been freely given and would thus be without substance.

2.3.2 Could the use of a contact tracing app be imposed by national law?

While the general prohibition on storage of and access to data, laid down in Article 5 E-Privacy Directive, does not leave room for a national obligation to use contact tracing apps, Article 15 E-Privacy Directive could provide a suitable legal basis for Member States to introduce such an obligation. According to this provision, Member States may overcome the guarantees provided by EU personal data protection law to the users of information technology services provided that

- they do so by way of legislation;
- this is justified by the necessity to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system;
- this is a necessary, appropriate and proportionate measure within a democratic society to safeguard the above objectives;
- this is in accordance with the general principles of Community law, including the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union.

Interestingly, Article 15 does not list public health among the grounds allowing Member States to limit the guarantees granted to users of information society services – in this case, apps – by the E-Privacy Directive. Also, there are good reasons not to allow legitimate reliance on objectives of public law, other than those expressly listed, to restrict the guarantees offered by the E-Privacy Directive, and good reasons not to interpret the specified legal grounds (such as "public security") as encompassing "public health" for the purpose of Article 15:

In fact, according to the CJEU, the list of objectives established by Article 15 is exhaustive[30] and subject to strict interpretation.[31] First, Article 15 must be understood as a clause that enables Member States to derogate from a general obligation of EU law incumbent upon them, i.e. to ensure respect for the guarantees contained in the E-Privacy Directive. Accordingly, it needs to be interpreted strictly. Notably, "that provision cannot [...] permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless".[32] Secondly, the wording of Article 15 itself makes clear that the legislative measures must be justified on one of the grounds laid down in Article 15(1), thus excluding that additional grounds can be legitimately relied upon[33].

[30] Judgement of 21 December 2016, Tele2 Sverige, joined Cases C-203/15 and C-698/15, EU:C:2016:970, para. 90; opinion of A.G. Sánchez-Bordona of 15 January 2020, Ordre des barreaux francophones and germanophone and Others, C-520/18, EU:C:2020:7, para. 34.
[31] Judgement of 21 December 2016, Tele2 Sverige, joined Cases C-203/15 and C-698/15, EU:C:2016:970, para. 89.
[32] Judgement of 21 December 2016, Tele2 Sverige, joined Cases C-203/15 and C-698/15, EU:C:2016:970, para. 89.
[33] Judgement of 21 December 2016, Tele2 Sverige, joined Cases C-203/15 and C-698/15, EU:C:2016:970, para. 90

3 Conclusions

Contact tracing apps are not *per se* incompatible with the EU privacy and data protection framework. However, based on our analysis of the applicable law, a few legal boundaries can be identified.

First, the legitimacy of a location data recording app, which the EDPB and the Commission have strongly argued against, can be ruled out. This is due to the presence of a more personal data protection-friendly alternative, i.e. proximity recording apps.

Secondly, a proximity recording app can operate without personal data, thus making the related data processing fall out of the scope of the GDPR. The E-Privacy Directive, instead, applies and requires the previous consent of the user for the app to store information on his smartphone or to access information already stored on his smartphone. This consent must be "freely given" by the app user and thus cannot be obtained by Member States by making the right to the movement of persons conditional upon the use of the app.

Finally, the necessity of the user's freely given consent for the full functioning of the app rules out that Member States can impose its use, nor does the E-Privacy Directive suggest that they are empowered to do so based on public interest considerations.