Hughes Hubbard & Reed

Guidance from the EDPB and the CNIL for GDPR-Compliant Covid-19 Contact Tracing

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

April 17, 2020 - On March 16, Andrea Jelinek, Chair of the European Data Protection Board (EDPB), said that *"Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects."*

The French government is examining technological initiatives as a means of combatting the spread of the coronavirus. The EDPB and the French Data Protection Authority (CNIL) have issued guidance on these specific issues in line with the GDPR and French legislation.

The Covid-19 outbreak has made recommendations on the topic of geolocation and other tracing tools the EDPB's highest priority. For this reason, the EDPB has deferred the issue of guidance on remote working tools and practices, and mandated its group of technology experts instead to study the effectiveness of location data aggregation and anonymization techniques.

The tracing tool in France : "StopCovid"

In France, a "StopCovid" contact tracing application is being developed by Inria, the *Institut national de recherche en sciences et technologies du numérique*. Its aim is to limit the spread of coronavirus by identifying persons who may have come into contact with an infected person. Once installed on smartphones, the application would make it possible to trace the history of close contacts between individuals over a certain period of time in the form of a reference ID, and if an individual tests positive for covid-19, anyone who has been in contact with him or her over a given period of time will be notified automatically. Exactly how the StopCovid application would function is not yet known.

In his speech on April 13, 2020, French President Emmanuel Macron confirmed that the application studied by the government would operate on an "anonymous and voluntary" basis and stated that *"the competent authorities will be able to enlighten us, as we cannot allow this epidemic to weaken our democracy or encroach on certain freedoms."*

GDPR-compliant StopCovid application

StopCovid's compliance with the GDPR can only be determined once its full functioning and specific characteristics have been revealed, even if some initial difficulties have already come to light, following its technical and legal evaluation:

- **StopCovid: a voluntary application**

In order for this "voluntary application" to be able to sufficiently cross check data, it will need to be used by more than 60% of the French population. However, according to an Ifop poll published on April 12, 53% of those polled said they were opposed to installing the application on their phones. Any consent obtained must comply with the requirements of the GDPR, including being express, free and informed.

- **StopCovid: an anonymous application**

The principles of data protection do not apply to anonymous information or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable.

StopCovid will apparently only use anonymous (non-identifying) data to the extent that the Bluetooth technology only uses radio waves and does not use personal data such as GPS location data of individuals. Effectively, proximity tracking would allow the identification of devices nearby without revealing the identity of individuals. However, at this stage, due to lack of knowledge as to the precise functioning of this application, it is not possible to confirm whether or not the data processed will be truly anonymous, i.e., that it will not be able to identify or allow the identification of individuals. Furthermore, if the data is not originally captured in anonymous form, but is anonymized (made anonymous), at any one stage, it cannot be excluded that the data will not be anonymous. Anonymization of data implies that use of an anonymization process aimed at eliminating any possibility of re-identification and personal data processed prior to the anonymization process, and will therefore have to comply with data protection legislation.

- **StopCovid: application accuracy and efficiency**

Bluetooth technology, although more privacy-protective than technologies based on location data, was not created for contact tracing. It requires user activation. It will therefore be necessary to assess the accuracy of the Bluetooth protocol to detect contacts over a certain period of time and distance, and it will need to be compatible with all possible versions of telephones.

Guidance from the chair of the CNIL

The CNIL has not been consulted to assess the conformity of the StopCovid application with the GDPR. On April 5, the chair of the CNIL, when questioned by the French press as to what the CNIL would pay attention to if it were asked to evaluate a tracing tool, responded:

- its **temporary** nature;

- its **compliance with data protection principles**, including:
  - using an identifier rather than personal data, and encryption rather than connection history,
  - being based on the free and informed consent of the user, and the absence of consequences for a user that refuses to download the application, and in the absence of consent, the fact that the application must be authorized by law; and
- the fact that the application has given rise to **careful analysis of its technical conditions.**

The CNIL Chair also specified that an application using Bluetooth technology would provide better guarantees than an application that specifically and continuously geolocates people.

On April 8, 2020, the chair of the CNIL was interviewed by the French Parliament and declared that *"Regulations that protect personal data do not oppose the implementation of digital tracking tools, individualized or not, for the protection of public health. Essentially, regulations require the provision of appropriate guarantees, which are all the stronger as the technologies are intrusive."* In this interview, the CNIL also summarizes recommendations on tracing tools using location data (GPS) which fall under a dual legal framework, the ePrivacy and the GDPR.

Audition commission des lois Assemblée nationale ; Propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL, April 8, 2020.

Guidance from the EDPB

The European Commission sought the advice of the EDPB on the draft guidance on apps assisting with combatting the Covid-19 pandemic. In a letter from the chair of the EDPB to Olivier Micolis, the head of the Data protection unit within the Directorate General for Justice and Consumers of the European Commission, adopted on April 15, 2020, the chair of the EDPB confirmed that it is preparing additional guidance to be released next week, notably on tracing and remote working.

In this letter, the EDPB has notably indicated that at this stage, it can only focus on the overall goal of the envisaged apps, and that:

- the development the apps should be documented with a **data protection impact assessment** and include **privacy by design** and **privacy by default** mechanisms;
- the **source code** of the apps should be made publicly available for the widest possible scrutiny by the scientific community;
- it is supporting a **voluntary adoption** of such apps *"a choice that should be made by individuals as a token of collective responsibility. It should be noted that voluntary adoption is associated with individual trust"*;
- the two **relevant legal bases** for the processing are:
  - the necessity of performing a task carried out in the public interest when public authorities provide the service; and
  - the necessity of complying with national law when a law promoting voluntary use and the absence of a negative impact on an individual who may refuse the use of the app, has been enacted;
- contact tracing apps **do not require location tracking of individuals users** because *"the main function of such apps is to discover events [...] which are only likely and for the majority of users may not even happen, especially in the de-escalation phase [a general reduction on the spread of the virus]. Collecting an individual's movements in the context of contact tracing app would violate the principle of data minimization"*;
- **Health authorities and scientists** should define some of the functional requirements of the app;
- Contacts with positive persons can be stored on local data storage within the individual's device or centralized storage *"provided that adequate security measures are in place, and that different entities may also be considered as controllers depending on the ultimate objective of the app"*, and the **decentralized solution is more in line with the data minimization principle**;

- The purpose of the app would be (according to the European Commission) *"for public health authorities to identify the persons that have been in contact with a person infected by COVID-19 and ask him/her to self-quarantine, rapidly test them, as well as to provide guidance on next steps, if relevant, including what to do if developing symptoms"*;
- Information provided to individuals via notification should be provided in such a way that the application **only processes random pseudonyms**;
- A mechanism should ensure **information** entered in the app according to which a person has tested positive, **must be correct and could be based on a one-time code** that can be scanned by the person using the test result;
- **Individual contact must only be performed by health authorities** after assessing strong data evidence and with the least amount of reference i.e, inductive, deductive, probabilistic or abductive reconstitution of personal data;
- **Algorithms** used in the app cannot be fully automated but **supervised by a qualified person**, notably using a call-back mechanism;
- **No element identifying any other data subject** should be contained in the app and the app should **not allow re-identification of any other data subject** *"the EDPB strongly suggests not to store any directly identifying data in user's device and that such data be in any case deleted as soon as possible"*.

Statement by the EDPB on the processing of personal data in the context of the COVID-19 outbreak, March 15, 2020; EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, April 14, 2020 (adopted on April 15, 2020).

Click here to go to our COVID-19 Resource Center for more advisories, articles and other content related to the coronavirus pandemic.

Related People

Stefan Naumann

Elsa Malaty

Related Areas of Focus

Data Privacy & Cybersecurity