Hughes Hubbard & Reed

Use of Contact Tracing Tools in the Context of Covid-19 Outbreak: the EDPB Guidelines

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 24, 2020 - The European Commission has asked EU Member States to develop a common EU approach for the use of mobile applications enabling citizens to take social distancing measures and to warn, prevent and contact trace to help limit the spread of coronavirus.

At present, the EU Member States are developing different smartphone applications to manage easing lockdown policies. These applications use a range of technologies from Bluetooth to geolocation data and artificial intelligence. But all have the goal of tracing contacts between people in order to break contamination chains as early as possible and/or map the spread of coronavirus.

The French government is working on a "StopCovid" app and has publicly announced this would be "anonymous and voluntary," using Bluetooth technology and not location data. On April 10, Apple and Google announced a partnership "to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus".

On April 21, 2020, the European Data Protection Board (EDPB) adopted guidelines on using location data and contact tracing tools in which it states that that the GDPR principles *"must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19."*

These guidelines provide practical guidance for GDPR-compliant Covid-19 contact-tracing tools.

- **General guidance**

The purpose of contact tracing tools is to notify individuals that they have been in close contact with someone who may be a carrier of the virus, in order to break contamination chains as early as possible. In contrast, location data is used to model the spread of coronavirus to assess confinement measure effectiveness.

In relation to contact tracing, the EDPB advises the following:

- **data protection impact assessments (DPIAs) must be carried out** before implementing such apps and the DPIAs must be published;
- **installation of such apps must be voluntarily** and individuals refusing to use them should not suffer any disadvantage;
- if the contact tracing app involves processing data already stored in the terminal and strictly necessary to provide the service explicitly requested by the user, the app provider would **not require user consent. However, if data processing** is not strictly necessary, the app provider **would need consent**;
- individuals must be clearly informed of the **controller's identity** from the outset and national health authorities could be controllers. The controller, in collaboration with the public authorities, must clearly and explicitly provide information on the download link for the official national contact tracing app to mitigate the risk of use of third-party apps;
- the **purpose of the apps must be defined**, *i.e.* it must be specific enough to exclude further processing for purposes unrelated to Covid-19 and must be necessary to ensure that the use of personal data is adequate, necessary and proportionate;
- careful consideration should be given to the **GDPR principles** of data minimization and data protection by design and by default. The app should not collect unrelated or unnecessary information such as civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers and *"data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals"*;
- contact tracing apps **do not require tracking the location of individuals**; instead, **proximity data should be used**;
- contact tracing apps **can function without direct identification of individuals and prevention measures must be used**;
- the **information collected must remain on the user's terminal** and only relevant information may be collected when absolutely necessary
- **algorithms** for such apps must be **strictly supervised by qualified personnel, not be based on automated processing, auditable and regularly reviewed by independent experts**;
- such apps' **source code should be publicly available** for the widest possible scrutiny;
- **ability to correct** data and/or subsequent analysis results is a necessity and data must be processed and/or stored in a way where such correction is technically feasible;
- **centralized and decentralized approaches are viable options**, provided there are adequate security measures in place and after carefully weighing up the effects on data protection /privacy and the possible impacts on individuals' rights;
- **servers involved in the contact tracing system must only collect** contact history or pseudonymous identifiers of a user diagnosed as infected following a proper assessment by health authorities and the voluntary action of the user. Alternately, the server may only keep a list of pseudonymous identifiers of infected users or their contact history for the time needed to inform potentially infected users of their exposure, and should not try to identify potentially infected users;
- **state-of-the-art cryptographic techniques** must be used to secure data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between an application and the server is also required; and
- **reporting users as Covid-19 infected on the app must be subject to proper authorization**, such as via a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. **If a secured confirmation cannot be obtained, no data processing presuming validity of the user's status should occur**.

The EDPB guidelines also contain analysis guidance on contact tracing apps to provide general guidance to designers and implementers of contact tracing apps.

- **Guidance on the relevant legal base for the processing**

The EDBP emphasizes that the voluntary basis of the app does not mean that consent is necessarily the legal basis for processing.

Apart from GDPR-compliant consent from the user, the necessity of performing a task in the public interest forms the relevant legal basis when public authorities provide a service required by EU or Member State's law to which the controller is subject.

Such EU or Member States law must explicitly indicate (i) the purpose of the processing and limitation of further unrelated use, (ii) that processing is necessary to perform a public interest task, (iii) that the app must be operated on a voluntary basis, (iv) a clear identification of the controller(s), and (v) criteria to determine when the app will be dismantled and who is responsible for and accountable for such determination.

- **Guidance on the lawful processing of health data**

Such app may involve processing health data in accordance with the GDPR when the **app user has explicitly consented to processing his health data for the specified purpose** (except if EU or Member States law prohibits such processing based on consent), or if the processing is necessary for:

- **reasons of public interest in the area of public health** on the basis of EU or Member States law, providing for suitable and specific measures to safeguard data subject's rights and freedoms, or
- i) purposes of preventive or occupational medicine, (ii) assessment of an employee's fitness, (iii) medical diagnosis, (iv) provision of health or social care or management of health or social care systems and services, on the basis of EU or Member State law or pursuant to contract with a health professional.

- **Guidance on data storage**
  The EDPB advises that personal data should only be kept during the Covid-19 crisis, and then deleted or anonymized.

EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on April 21, 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