GIBSON DUNN

April 28, 2020

EUROPEAN PERSPECTIVE ON TRACING TOOLS IN THE CONTEXT OF COVID-19

To Our Clients and Friends:

As part of the fight against the spread of COVID-19 and desire to effectively lift the lockdown, governments and private companies around the world are considering the use of data driven digital tools, in particular digital tracing solutions.

Such tracing technology may serve multiple purposes; among the main ones are: (i) collecting mobile location data in order to model the spread of the virus and measure the effectiveness of confinement measures; and (ii) contact tracing, in order to alert individuals that they have been in close proximity of someone who has tested positive for COVID-19.

Various initiatives to develop tracing solutions are currently being pursued, including both public and private initiatives, which praise the merits of tracing solutions that have been rolled out successfully in Asia-Pac. The use of such tracing tools in the context of the pandemic requires the collection of personal data such as health data and potentially location data, which has prompted data protection authorities in Europe to alert on the need to comply with fundamental privacy rules set forth in the GDPR[1] and the ePrivacy Directive[2]. Debates have sparked in various European jurisdictions on how to conciliate the use of digital tracing solutions - which could be perceived as intrusive - and the need to guarantee individuals' rights such as privacy and data security.

In order to help European countries navigate through these complex issues, on April 21, 2020 the European Data Protection Board ("**EDPB**") adopted its guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak ("**Guidelines**").[3]

This Client Alert summarizes the key privacy implications of collecting personal data through tracing tools in Europe.

1. Positions and Guidance of the EU Institutions regarding COVID-19 Tracing Applications

Since the beginning of the pandemic, the European Commission and its various institutions have been supportive of private and public initiatives for the creation of tracing applications capable of contributing to the containment of COVID-19. The European Commission has actually drafted an inventory of the initiatives carried out in Europe and worldwide to develop and offer digital tracing tools in response to the COVID-19 pandemic[4].

However, the use of data intensive technologies and applications, as well as the artificial intelligence underpinning such applications, have also raised concerns from a data privacy and cybersecurity perspective, which have led both the European Commission and the EDPB to adopt guidelines:

- Taking the GDPR and the ePrivacy Directive as references, the European Commission and the EDPB have started to publish their opinions on the compliance of tracing applications with EU privacy and cybersecurity rules in mid-March and throughout April. The EDPB insisted first on the fact that the GDPR should not hinder the capacity of the EU Member States to fight the pandemic through the processing of mobile location data, provided that such data were anonymized and collected in an aggregated manner.[5] The European Commission published its guidance on applications[6] setting out the main requirements that applications shall meet to ensure compliance with data protection regulations (e.g., retention of control by users, applicable legal basis, data minimization principle). The European Commission further indicated in its guidance that app developers should aim to exploit the latest privacy-enhancing technological solutions, such as Bluetooth proximity technology, in order to provide contact tracing features without allowing applications to track individuals' locations.

- Based on the European Commission's guidance, the EDPB finally adopted its Guidelines on April 21, 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.[7]

  The EDPB emphasized that preference should always be given to the processing of anonymized data rather than personal data of identified or identifiable persons. It also reminded that anonymization[8] processes have to comply with strict requirements and pass the "*reasonableness test*", which considers the effectiveness of anonymization tools taking into account both objective aspects (e.g., technical means to re-identify individuals) and factual elements (e.g., nature and volume of data involved that would need to be process to re-identify individuals).

  As to the use of tracing tools, the EDPB confirmed that the use of contact tracing applications should be voluntary. Accordingly, in order to ensure that individuals have a real choice, those who decide not to (or cannot) use such tracing applications should not suffer any negative consequence derived from that decision or situation. In the words of the EDPB, individuals must have full control over their personal data at all times, and should be able to choose freely to use any application.

  The EDPB also recalled general data protection principles that should be complied with in this context, notably:

  Accountability: The EDPB indicates that the controller of the contact tracing application should be clearly identified. In this respect, it considers that national health authorities could act as controllers for applications developed by public administrations, but other controllers may also be envisaged.

Purpose limitation: The Guidelines specify that the purposes aimed by tracing applications should exclude objectives or uses of data that are unrelated with the management of the COVID-19 crisis (for example, commercial purposes).

Data minimization and principles of privacy by design and by default: According to these GDPR principles, any personal data processed should be reduced to the strict minimum. Rather than collecting and sharing location data via the application, contact tracing applications should be based on proximity communication technologies that enable the broadcasting and receipt of data among users (e.g., proximity data based on Bluetooth Low Energy). The EDPB recommends that this data should be subject to regular pseudonymisation, and that measures should be implemented to prevent re-identification.

Lawfulness of processing: Different legal bases are considered by the EDPB depending on the data collected and the entity providing the application (e.g., consent, performance of a task for public interest). The choice of the most appropriate legal basis will largely depend on whether an application is developed and offered by private parties or by public administrations.

Storage limitation: The Guidelines recommend that personal data should be erased or anonymized immediately after the COVID-19 crisis.

Data security: The EDPB recommends to use pseudonymous identifiers and state-of-the-art cryptographic techniques to ensure data security.

Finally, the EDPB considers that a data protection impact assessment shall be carried out before implementing a tracing tool, as the data processes involved in the functioning of such an application are likely to result in a high risk to the rights and freedoms of individuals.

As an annex to these Guidelines, the EDPB provided practical guidance to app developers and users of contact tracing applications. For example, we note that the source code of the application and of its back-end should be open.

It is worth mentioning that the EDPB adopted two letters on April 24, 2020 in response to members of the European Parliament[9]. In its letters, the EDPB notably reminded that data protection law already enables to implement data processing necessary to fight an epidemic and that "*there is no need to lift GDPR provisions but just to observe them*". The EDPB mainly referred to its recently adopted Guidelines and specified that it has taken into account concerns from the stakeholders involved as well as the general public when drafting such Guidelines.

2. Specific Positions of Member States regarding COVID-19 Tracing Applications

Certain EU Member States and other states from the European Economic Area have already implemented tracing tools in their respective territories (e.g., in Austria, Czech Republic, Iceland, Poland). While other EU Member States are currently still considering the development and roll-out of tracing applications, the conditions under which such applications would contribute to the fight against the COVID-19 have not been clearly established yet.

In this context, EU Member States' Data Protection Authorities ("**DPAs**") have also issued their own opinions in recent weeks, applicable to applications used in their respective territories. While these DPA opinions should follow and be based on the basic principles set at EU level, each DPA has taken a unique position on the various data privacy implications of tracing tools in its own EU Member State.

- ***Belgium***

In Belgium, the main initiative to develop a contact tracing application has come from the public administration. By mid-April, it was reported that the Belgian State was working on a public application that would enable the tracking of infected individuals and the issuing of warnings to other individuals who would have crossed infected persons within a period time. However, reporting to the press on April 23, 2020, the Belgian Minister of Digital Agenda indicated that Belgium no longer needed, for the time being, an application for automated contact tracing. Instead, the Minister expressed a preference for confinement rules and for manual tracing by health services. To support its position, the Minister also referred to the high utilization rate that a tracing application would require to ensure its effectiveness (60%), and the low download rates that had been recorded in other European countries where an application had already been launched (e.g., in Austria, where only 400,000 downloads had been registered in a country with a population of 8.9 million people – i.e., a 4.5% usage rate).

Notwithstanding the position adopted by the Belgian Government, on April 8, 2020 the Belgian Data Protection Authority ("**Belgian DPA**") published a press release[10] emphasizing basic principles for the processing of personal data by contact tracing applications. First, the Belgian DPA recommends not processing any personal data if this is not required to offer the services to the users (e.g., name, e-mail address, mobile number). However, the provision of certain applications implies necessarily the processing of personal data in order to offer the service (e.g., IP addresses). In such situation, applications should only process personal data to ensure their appropriate functioning in light of the objective pursued. Any data inputted may continue to be processed by the app provider depending on whether the user intends the service to continue after it finishes using the application.

- ***France***

On April 24, 2020, the French DPA ("**CNIL**") adopted a decision on the project of mobile application "StopCovid"[11] initiated by the French government, which is a contact tracing application based on Bluetooth technology (not using geolocation technology).

First, in accordance with the purpose limitation principle, the CNIL notes that the tracing tool may only be used to inform its users in the event of contact with an individual tested positive for COVID-19 but not for other purposes like monitoring the compliance of confinement measures. Besides, the CNIL welcomes the fact that the intended tool would be based on a voluntary approach. As recommended by the EDPB Guidelines, the CNIL reminds that individuals who decide not to download/use the "StopCovid" application should not suffer any negative consequences (such as a prohibition to take public transportation).

With respect to the lawfulness of the processing, again in line with the EDPB Guidelines, the CNIL estimates that the performance of a task of public interest would be the most appropriate legal basis when

the processing is carried out by public authorities (Art. 6-1-e of the GDPR). For the specific processing of health data, the CNIL considers that the processing carried out in the context of the "StopCovid" application would be necessary for reasons of public interest in the area of public health (Art. 9-2-i of the GDPR). Having this in mind, the CNIL recommends that the use of a voluntary contact tracing application should be governed by a specific legal provision in French law.

In addition, the authority reminds the principles of data minimization and storage limitation according to which the data shall be kept only for the use of the application. Finally, the CNIL provided specifications on the application configuration. As to the accountability principle, the authority estimates that the controller should be the French Health Ministry or any other health authority involved in the health crisis management. It also reminds the necessity to carry out a data protection impact assessment, as recommended by the EDPB. The importance of data accuracy and data security as well as the respect of data subjects' rights should also be taken into account.

The French Parliament will debate, in the upcoming weeks, on whether or not to implement this application. After the debate, if it is decided to deploy the application, the CNIL has requested to be consulted again in order to give its opinion on the final arrangements of the application "StopCovid".

- ***Germany***

In Germany, one initiative emerged that initially garnered the strongest State support: the **Pan-European Privacy-Preserving Proximity Tracing ("PEPP-PT")** initiative[12]. Composed of a consortium of over 130 members, including telecommunications operators, health service providers, scientists and other relevant actors and stakeholders, the PEPP-PT initiative was created on March 31, 2020 in order to develop and offer a tracing technology that would be compliant with EU privacy and data protection rules and would be effective in the contention efforts of States against COVID-19. However, the PEPP-PT initiative recently suffered strong criticism given its centralized structure, which requires users to upload contact logs to a central reporting server, thereby allegedly exposing users to direct State control.[13] The PEPP-PT protocol is allegedly supported by the UK, France[14] and, until recently, Germany.[15]

Another initiative, **Decentralized Privacy-Preserving Proximity Tracing ("DP-3T")**, has also garnered strong support in the EU. Backed by Switzerland, Austria and Estonia,[16] in cooperation with companies such as Apple and Google, DP-3T would reportedly abide more strictly by the guidance offered by EU authorities, in particular regarding the reliance on proximity data technology and the absence of tracking of location data. Its decentralized structure does not require users to upload contact logs (which remain in the users' device), and the processing of data to inform users of contacts with infected individuals occurs locally. Further, under the decentralized DP-3T approach users may opt to voluntarily share their phone number and details of their symptoms with the authorities, but this would not automatically occur as opposed to the centralized structure of the PEPP-PT initiative.

Germany has been one of the main supporters of the PEPP-PT initiative until April 26, 2020, when it backed away from a centralized approach in favor of a decentralized system architecture.

The German data protection commissioner[17] indicated on his website that contact tracing tools should be implemented in a transparent manner and on a voluntary basis. According to the commissioner, an individual tracking or a later re-personalization should be excluded.

- ***Spain***

In Spain, regions like Madrid, Catalonia, Basque Country and Valencia, have offered publicly-sponsored applications to trace infected individuals. Based on the tracing application developed by the Madrid Region, the Spanish Government launched the nation-wide application, initially covering a limited number of regions. These applications aim at tracing users and their contacts in order to alert them of potential COVID-19 contagion and spread. However, the overlapping uses of the different applications and their limited success (not exceeding 10% of the population in the respective regions) have put their effectiveness into question. Recently, it was reported that Spain is participating in the PEPP-PT initiative, although it is unclear if this position will shift to the DP-3T initiative, backed by other Member States. As soon as the technology would become available, Spain would require the cooperation of both public administrations and private entities to launch the automated tracing application[18].

On March 26, 2020, the Spanish Data Protection Agency ("**AEPD**") published a communication on self-evaluation and contact tracing applications to fight COVID-19[19]. While the AEPD acknowledged that the GDPR and Spanish data protection rules cannot serve as an obstacle to limit the effectiveness of any measure, it reminded that fundamental data protection and privacy rights still needed to be complied with. As regards the legal bases available to offer contact tracing applications, the AEPD indicates that data processing by national and regional health authorities may be carried out in the public interest and to protect the vital interests of the individuals. Applications developed and operated by private entities need to rely on another legal basis in order to process personal data (e.g., consent).

Any data collected may only be processed for purposes related to the control of the COVID-19 epidemic (e.g., to offer information on the use and control of the self-evaluation applications or to obtain statistics with aggregated geolocation data to offer maps that inform users on high/low risk areas). The AEPD also reminded app developers that parental authorization shall be required for users aged below 16.

- ***United Kingdom***

The United Kingdom DPA ("**ICO**") published, on April 17, 2020, an opinion[20] on the Apple and Google joint initiative (called the Contact Tracing Framework) to enable the use of Bluetooth technology to help governments and public health authorities reduce the spread of the virus. The ICO indicates that the proposals for this initiative appear to be aligned with the principles of data protection by design and by default. It also specifies in its opinion that organizations designing contact tracing applications are responsible for ensuring that the application complies with data protection law and that such organizations are acting as controllers.

The ICO also published a series of questions[21] to be taken into account to ensure that privacy concerns are properly considered when using digital tracing tools.

Finally, it is worth noting that the ICO revealed[22] that it has been working with the National Health Service ("**NHS**") in the context of the development of a contact tracing application in order to help them ensure a high level of transparency and governance. The NHS has emphasized its commitment to transparency, security and privacy and its collaboration with health data privacy stakeholders and advisers in developing the application[23]. However, the NHS's proposed application is different from the Apple-Google model, in particular by using a structure centralized within the NHS, meaning that the matching process, which works out which phones to send alerts to, happens on a computer server rather than decentralized on handsets, to record infections and send out alerts. While it is hoped that this will make it easier for the NHS to notify people appropriately and adapt the system as knowledge improves, there may be a trade-off in terms of the central repository's vulnerability to hackers.

***

As can be seen, the EU institutions, the EDPB and the EU Member State DPAs have published their guidelines and made clear the red lines that should be complied with in preparing and offering contact tracing tools. Regardless of whether they result from public or private initiatives, these rules and principles enshrined in the GDPR should drive the development and offering of contact tracing tools.

The effectiveness of contact tracing applications relies on its wide adoption by users in a territory, which largely depends on the strength of the State sponsorship received or the ability of companies to advertise its use.

From a technical standpoint, research projects and initiatives like PEPP-PT and DP-3T have emerged which aim at developing national applications based on a standardized approach. The infrastructure of the tools that are being developed under such protocols, centralized or decentralized, may come under scrutiny by the European Commission and the DPAs. However, given the importance of State sponsorship in the adoption of protocols for particular territories, and the apparent divergent approach followed by different EU Member States, it is likely that both protocols will co-exist within a non-harmonized EU approach.

We will continue to monitor privacy and cybersecurity developments related to COVID-19 in Europe and around the world, and will provide further communications as developments warrant. Gibson Dunn's lawyers are also available to assist with any questions you may have regarding privacy implications of tracing tools in the United States.

---

[1] 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.

[2] 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.

[3] 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.

[4] Commission's Inventory Mobile Solutions against COVID-19.

[5] EDPB Statement on the processing of personal data in the context of the COVID-19 outbreak adopted on March 19, 2020.

[6] Commission Guidance of April 17, 2020 on Apps supporting the fight against COVID 19 pandemic in relation to data protection. Please note that considering the urgency of the current situation, these guidelines will not be subject to public consultation.

[7] 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.

[8] The EDPB defined anonymization as "*the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable individual against any "reasonable" effort*".

[9] Letter of the EDPB to Sophie in't Ved dated April 24, 2020; Letter of the EDPB to Mrs Ďuriš Nicholsonová and Mr Jurzyca's dated April 24, 2020.

[10] Publication on the website of the Belgian DPA.

[11] Decision n° 2020-046 of April 24, 2020 adopting an opinion on the project of mobile application "Stop Covid".

[12] Website of the PEPP-PT.

[13] Website of Ouest France.

[14] Reuters, *Germany flips to Apple-Google approach on smartphone contact tracing*, News Report dated April 26, 2020.

[15] Statement by Helge Braun, Minister of the Chancellery, and Jens Spahn, Federal Minister of Health, on the tracing app, Press Release dated April 26, 2020 (available in German).

[16] *Supra* note 13.

[17] Publication on the website of the Federal Commissioner for Data Protection and Freedom of Information dated April 22, 2020 (available in German).

[18] Publication on the website of El Pais dated April 14, 2020.

[19] Publication on the website of the Spanish Data Protection Agency dated March 26, 2020.

[20] ICO's Opinion: Apple and Google joint initiative on COVID-19 contact tracing technology dated April 17, 2020.

[21] ICO's Blog: Combatting COVID-19 through data: some considerations for privacy dated April 17, 2020.

[22] ICO's Statement in response to details about an NHSX contact tracing app to help deal with the COVID-19 pandemic dated April 24, 2020.

[23] NHS Blog: NHSX: Digital contract tracing: protecting the NHS and saving lives dated April 24, 2020.

The following Gibson Dunn lawyers prepared this client update: Ahmed Baladi, Alexander Southwell, Patrick Doris, Michael Walther, Vera Lukic, Alejandro Guerrero, Clémence Pugnet, Selina Grün, Sarika Rabheru and Charlotte Fuscone. Gibson Dunn lawyers regularly counsel clients on the privacy and cybersecurity issues raised by this pandemic, and we are working with many of our clients on their response to COVID-19. Please also feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the ***Privacy, Cybersecurity and Consumer Protection Group****:*

United States

Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)

Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)