HERBERT SMITH FREEHILLS

COVID-19: PEOPLE: WHEN PUBLIC HEALTH AND PRIVACY COLLIDE? (GLOBAL)

18 March 2020 | Global
Legal Briefings

SUMMARY

- Governments and public authorities globally are requiring increased access to personal data of citizens in order to attempt to control and monitor the current spread of COVID-19.
- The pandemic is generally recognised by data protection authorities as giving rise to extraordinary circumstances, although in Europe at least there are still requirements for processing to be necessary and proportionate, and for personal data to be adequately protected.
- Governmental responses around the world appear to be in some instances creating a tension between public health on the one hand and privacy on the other, highlighting a new and possibly unexpected consequence of current unprecedented times. When the crisis is over, nation state approaches to privacy may need to be reconsidered and re-evaluated.

THE PAN-EUROPEAN PERSPECTIVE: THE EDPB STATEMENT

On 16 March 2020 the European Data Protection Board ("EDPB") released a statement on measures taken to contain and mitigate COVID-19. The EDPB stated that data protection rules "*do not hinder measures taken in the fight against the coronavirus pandemic*". This includes the General Data Protection Regulation ("GDPR") which enables personal data processing without obtaining consent where it is in the public interest or the vital interests of any natural person.

The EDPB recognised that "*even in these exceptional times*" every controller must ensure that personal data is protected, and that the lawful processing of personal data must be guaranteed. All processing must be in the public interest and must be proportionate to the legitimate aim pursued. Further, the general principles surrounding data processing including transparency still apply, except where necessary and proportionate for reasons of national security.

TENSION BETWEEN PUBLIC HEALTH AND PRIVACY?

Around the world, governments have attempted to control the pandemic by harnessing new technology and its power to collect and analyse increasingly large amounts of data, including personal data, which are generated on a daily basis in our societies. Whilst it is understandable that governments are seeking to use all means at their disposal in order to control the pandemic, there is a natural tension between the use of this data and the protection of personal privacy rights. Globally, a wide range of approaches have been taken and variety of statements made which either re-affirm a commitment to data privacy, or conversely, appear to back-track on previous approaches.

Some examples of this tension currently being reported on the global stage in response to the COVID-19 crisis include:

- The approval of emergency measures in Israel which allow the use of technology developed for counterterrorism purposes to track infected persons by monitoring their mobile phones. This monitoring technique could be used to notify people who have come into contact with infected persons or enforce quarantine orders.

- The use of facial recognition and thermal scanning technology, in combination with passenger rules requiring people using public transport to use their real names in China. Data is shared with the police and with media outlets who report on patients' travel history, which could include where they sat on a train or which compartment they boarded on the subway.

- The GPS tracking app and SMS alert system used in South Korea where public authorities send text messages detailing the age, gender and recent movements of anyone recently diagnosed. This approach caused issues when speculation on the whereabouts of various infected persons broke out online.

- The extensive powers put in place by the data protection authority in Italy until at least

30 July which allow civil protection personnel to process data including special category data and communications between employees.

- The rules put in place by the US Department of Health and Human Services in the USA requiring airlines to collect and provide extensive data for passengers on certain flights.

CONTACT TRACING

Contact tracing refers to the way that governments identify and monitor infected persons, which often means collecting location data. In the EU, national laws implementing the ePrivacy Directive only allow use of location data when made anonymous. Emergency legislation can be passed but only where '*necessary, appropriate and proportionate within a democratic society'*, and where adequate safeguards are put in place. In this respect, it will be interesting to monitor the responses of the various Member States' governments to see if any such legislation is passed.

A number of countries worldwide are using location data to track and monitor anyone infected by the virus and those they have been in contact with. The USA, Iran, Singapore, Taiwan and Israel have all collected data from third parties or government-mandated apps which collect location data directly.

In addition, authorities in Germany, Ireland and Canada have indicated that they would be open to collecting and processing location data. When asked about the use of cell phone data in contact tracing investigations in Canada, the Ontario Premier commented that "*everything's on the table right now*". Ontario's Information and Privacy Commissioner stated in response that they would not challenge such a decision as long as any measures were correlative to the outbreak, as public health officials had the power to '*take extraordinary steps to keep the public safe'*.

LIMITATIONS ON DATA PROCESSING

Some public authorities are clear that powers to process personal data even as a response to the outbreak should not be unlimited. Data protection authorities in Ireland, France and Argentina have all released statements to the effect that public health authorities are entitled to collect and process health data without consent, but have stated that any measures taken must be necessary and proportionate and must not go beyond the management of suspected exposure to the virus. In particular, the Data Protection Commission in Ireland has made it clear that organisations must have regard to principles of transparency, security and accountability, and that only the minimum amount of data necessary should be processed.

Further, the Information Commissioner's Office (the "ICO") in the UK released a statement that, while data protection laws would not prevent data from being shared as a result of the pandemic and that the ICO recognises the "*unprecedented challenge*" of Coronavirus, any excessive or unlawful data processing will still be prohibited. However, importantly, the ICO appears to have taken a proportionate response, accepting that companies are dealing with an unprecedented event, and that whilst they cannot extend timescales which are enshrined in law, that the ICO will use its own channels to manage data subjects expectations and will take a measured and proportionate response in terms of any investigations. Finally, the ICO reiterates that, even though companies' working styles are changing and more and more employees will be working from home, that companies must still have regard to their technical and organisational security measures in order to protect personal data.

A GATEWAY TO INCREASED SHARING OF PERSONAL DATA?

Another consequence of the outbreak is that many government authorities have required private companies to share personal data originally collected for commercial purposes. Officials in Singapore have requested location data from airlines, taxi companies and ride-sharing apps such as Grab, while the USA have pressed airlines and hotels to provide extensive customer data even where Airlines for America have maintained that the requirements are "beyond the capabilities of airlines".

WHAT NEXT?

It certainly seems that COVID-19 is having and will continue to have an interesting relationship with global data protection legislation and the right to privacy enshrined (often recently) in many laws around the world. Whilst it does not yet appear that data subjects are raising challenges to the governmental responses, it is important to note that many regulators, particularly in Europe, are reiterating the need to keep data protection in mind when considering responses to this pandemic and, when the dust of the current crisis has settled, the impact on data protection and privacy may be an interesting and unintended consequence of today's unprecedented events.

More on navigating the COVID-19 Outbreak

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.


MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

LAUREN HUDSON
ASSOCIATE, LONDON

+44 20 7466 2483
lauren.hudson@hsf.com

LEGAL NOTICE