DATA PROTECTION IN A TIME OF COVID-19: GUIDANCE AND PRIVACY CONCERNS DURING A PANDEMIC

Data protection regulators across the world have published useful guidance on compliance and enforcement during the coronavirus outbreak. Meanwhile, governments are using tracking technologies to slow the spread of the virus, cyber criminals have increased their activities and businesses risk fines if they ignore data protection and privacy laws. This briefing recaps EU and UK guidance, and discusses government use of technologies to protect public health.

Guidance from data protection regulators

Data protection regulators across the globe are aware that these are difficult times, and have issued guidance accordingly. Even so, organisations cannot afford to be complacent.

A global list of local regulators and guidance is available on the Global Privacy Assembly website[1]. The Chair of the European Data Protection Board (EDPB), which oversees data protection and privacy across the European Economic Area, issued a statement on 19 March 2020[2]. In the UK, the ICO issued its own guidance[3].

Some common themes are as follows:

- **No hiatus from data protection obligations**. Organisations should continue to ensure that they comply with their obligations under applicable data protection and ePrivacy laws, including ensuring that they have the appropriate lawful grounds for processing personal data and special category personal data.
- **DSAR response enforcement.** In the UK, the ICO hints that, whilst it cannot extend statutory time limits and organisations must still respect individuals' rights, the ICO might not rush to penalise organisations struggling to respond to data subject access requests within the statutory thirty days.
- **Coronavirus emails.** Data protection and ePrivacy rules do not stop the Government, the UK NHS or other health organisations or professionals from sending public health messages. Reading between the lines, this is **not** an excuse for other kinds of organisations to raise brand awareness without complying with ePrivacy rules. Before sending out what could be seen as spam, organisations should check that either:
  - the communication really is essential in order to carry out the business; or
  - if not, that where using individuals' personal email addresses they have consent or the 'soft opt in' applies, i.e. that the messages are to existing customers who have been given the opportunity to unsubscribe from marketing. Organisations should not send non-essential messages to individuals who have already unsubscribed from marketing.
- **Cyber security from home.** Cyber criminals are seizing the opportunity to increase attacks. Organisations also need to ensure that they have sufficient security in place to cope with remote working systems.
- **Communicating with employees about infections.** The ICO clarifies that although it is permissible (and necessary) to tell staff that a colleague may have contracted coronavirus, organisations should usually not name the individuals in question. Health data are 'special category' personal data and as such require additional justification for processing. Organisations should share only the data which are strictly necessary to ensure the health and safety of their workforces and customers. Where it is necessary to disclose an individual's name in connection with coronavirus, organisations should inform the individuals in advance and treat them respectfully.
- **Lawful grounds of processing and accountability.** It may be possible in a human resources/ business context to rely on the lawful ground that processing is necessary for compliance with an employer's legal obligations, and/or for reasons of substantial public interest in the area of public health. However, organisations should not assume that a lawful ground or exemption applies without considering it carefully. The principle of accountability also still applies and organisations should keep careful file notes of their decisions.
- **Collect only relevant data.** In line with data minimisation principles, organisations should only collect the information that they actually need. For example, they will need to know if employees are experiencing coronavirus symptoms, and it is reasonable to ask people whether they have recently visited particular high-risk countries. However, organisations should exercise caution if collecting other health data, and should put appropriate safeguards in place to keep such data safe.
- **Sharing health data with authorities.** The ICO clarifies that if it really is necessary to share data about specific individuals with public authorities then data protection law will not prevent this.
- **Consent usually required for location data.** The EDPB points out that organisations must respect ePrivacy laws when processing telecom data such as location data (see discussion on tracking below). Local laws may vary on this, as the current EU ePrivacy Directive[4] is implemented by national laws in each EEA Member State. Organisations can usually only use location data with either consent from the individuals or where the data have been anonymised first. The exception is where EEA Member States introduce legislation permitting more widespread use. Such legislation must be *"necessary, appropriate and proportionate… within a democratic society"* and subject to appropriate scrutiny.

Tracking location data to combat coronavirus

Governments around the world are considering using mobile location data as a way to monitor, contain or mitigate the spread of coronavirus.[5] The European Union is likely to take a cautious approach to such monitoring, but in other parts of the world tracking is already taking place.

In China, the government reportedly worked with a number of tech giants

1 https://globalprivacyassembly.org/covid19/

2 https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

3 https://ico.org.uk/for-organisations/data-protection-and-coronavirus/

4 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).

5 https://privacyinternational.org/examples/tracking-global-response-covid-19

"Organisations should continue to ensure that they comply with their obligations under applicable data protection and ePrivacy laws, including ensuring that they have the appropriate lawful grounds for processing personal data and special category personal data."

to keep track of the population.[6] Media sources report that Map App provider Baidu created a layer on top of its standard maps to show real-time locations of confirmed and suspected cases of the virus, and Qihoo 360 launched a platform where travellers can check if anyone on the same transport recently tested positive. Baidu's technology, used in railway stations and airports, apparently uses artificial intelligence (AI) to direct an infrared sensor on the foreheads of moving passengers to detect their temperatures and report suspected cases.[7] In Hangzhou, media sources report an experimental system dubbed the Alipay Health Code which tracks individuals' compliance with quarantine rules.[8] The system works through Ant Financial's wallet app Alipay and assigns users a colour code indicating their health status (green, yellow or red). This works well in a number of cities where residents must register their phone numbers with an app in order to take public transportation, and where citizens must show their Alipay codes at a number of health checkpoints in order to travel around freely. Part of the software allegedly has the potential to report the person's location, city name and an identifying code number to the police. Ant Financial clarifies that it requires all third-party developers to obtain user consent before providing services. Manufacturer Telepower has apparently added fever detection and facial recognition to point-of-sale terminals used for catering, retail, payment, security and other applications.[9] In Hong Kong, individuals under compulsory home quarantine are being issued with tracker wristbands to help enforce isolation.[10]

China is not alone. Israel recently passed an emergency law allowing it to locate people who have been in contact with coronavirus sufferers.[11] In the USA, Clearview AI is allegedly negotiating a partnership with government agencies for similar purposes and Palantir, a data mining company, is reportedly already sharing data with the CDC and NIH.[12] Telecoms companies in various EEA Member States are sharing user data with the authorities, and in some cases working with companies such as Facebook to leverage big data.[13] In the UK, BT/EE is reportedly discussing sharing location and usage data with the government to help monitor public compliance,[14] and UK researchers are also working on an app to alert people who have come into contact with someone known to have coronavirus.[15]

The EDPB advocates a more cautious approach in Europe. The EDPB's statement[16] recognises the possibility of using mobile location data to track individuals or to send public health messages to individuals in a specific area by phone or text message. However, it strongly advises that public authorities *"should first seek to process location data in an anonymous way... which could enable generating reports on the concentration of mobile devices at a certain location"*. Whilst it recognises that EEA Member States

6 https://www.weforum.org/agenda/2020/02/coronavirus-chinese-companies-response/
7 https://www.techinasia.com/ai-surge-china-coronavirus
8 https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
9 https://privacyinternational.org/examples/3462/china-manufacturer-telepower-adds-fever-detection-and-facial-recognition-point-sale
10 https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html
11 https://www.bbc.co.uk/news/technology-51930681
12 https://www.biometricupdate.com/202003/governments-looking-into-advanced-surveillance-biometric-tech-to-contain-coronavirus
13 https://privacyinternational.org/examples/3421/facebook-italian-ministry-seeks-leverage-big-data-help-facebook-and-telcos
14 https://www.theguardian.com/world/2020/mar/19/plan-phone-location-data-assist-uk-coronavirus-effort
15 https://www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html
16 https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

are entitled to introduce legislative measures to safeguard public security, it points out that if this involves non-anonymised location data then the legislative measure must also put in place adequate scrutiny and safeguards. These could include providing the right to a judicial remedy. It also emphasises that governments should always use the least intrusive solutions possible, taking into account the specific purposes of the legislation. Blanket surveillance is unlikely to be compliant with EU laws.

Data protection and human rights organisations worry that the use of technology to track individuals on a large scale, even for important public health reasons, may open the door to intrusive monitoring in the long term.

Our take

In summary, regulators are fully aware of the struggles organisations and their governments are facing in the current climate, and when considering enforcement they will take into account the compelling public interest in the current health emergency. Having said this, the current climate is not an opportunity to flout the rules or abuse the rights and freedoms of individuals.

Public health interests can provide legitimate reasons to increase monitoring of individuals, but monitoring even by governments must be approached with caution. The latest developments in tracking technologies and AI could have serious implications for individuals' privacy long after the coronavirus pandemic has abated.

This is a time when individuals need more protection than ever. Organisations should be mindful of this when implementing new policies and procedures, or conducting new marketing campaigns. Regulators may be prepared to cut organisations some slack during this period, but now is not the time to be complacent.

For further information, please contact:

FELICITY BURLING
Associate
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

or your usual HFW contact.

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our data protection capabilities, please visit hfw.com/Data-Protection.

hfw.com

Americas | Europe | Middle East | Asia Pacific