

COVID-19: Three Data Protection Tips for the EU and the UK

March 23, 2020

As businesses adapt to the COVID-19 pandemic, the challenges of managing a remote workforce and its desire for information about the virus's impact have significant data protection implications. While European Data Protection Board ("EDPB") [guidance](#) confirms that the GDPR should not impede the fight against the pandemic, even in these exceptional times, companies must continue to safeguard individuals' data protection rights.

We share here our top three tips for those who oversee data protection compliance, drawing on guidance from the [EDPB](#), [UK](#), [French](#), [German](#) and [Irish](#) supervisory authorities. Links to other authorities' guidance are accessible [here](#).

Identify and Address New Data Security Challenges. With many employees now [working remotely](#), data security concerns need to be addressed as the requirement to maintain appropriate technical and organizational measures to safeguard personal data (**GDPR Articles 5(1)(f) and 32**) applies equally inside and outside the office. The UK Information Commissioner's Office's (the "ICO") COVID-19 [guidance](#) calls on companies to "*consider the same kinds of security measures for homeworking that you'd use in normal circumstances*".

Companies may therefore want to remind employees of the need to:

- prevent unauthorized access to personal data by family members, housemates or anyone else in the home by sharing, practical, easily implementable strategies such as putting work papers away at the end of each day out of sight;
- adhere to pre-existing data security rules while outside of the office. For example, employees should not use personal email accounts for work business even if remote access tools are under strain; and
- remain vigilant for hackers trying to exploit the crisis through phishing emails and other attacks, discussed further in our COVID-19 cybersecurity [checklist](#).

Collect, Share and Retain the Least Amount of Information Necessary. Collecting and sharing COVID-19–related data needs to be carefully considered. While the ICO [guidance](#) states that companies can lawfully keep staff informed about COVID-19 cases within the organisation, it reminds businesses to share information only when truly necessary.

The ICO suggests that naming affected individuals is unnecessary in most contexts and should be avoided. [Guidance](#) from the German Data Protection Conference (*Datenschutzkonferenz*), a group of federal and state data protection regulators, supports this approach, stating that the identity of an infected individual must be kept confidential unless there is no other way to take precautions to protect others. If naming an individual proves unavoidable, companies should document the reason and follow the EDPB [guidance](#) to inform the individual before their name is disclosed.

Companies must also be circumspect when collecting COVID-19–related information. Although few organizations will be receiving physical visitors for the time being, those which are should ask them to provide only the information truly necessary to protect the company’s workforce. The same applies to employees. The ICO [guidance](#) suggests that it is reasonable to ask people if they have visited specified countries affected by the virus or are experiencing COVID-19–related symptoms. Similarly, [guidance](#) from the French supervisory authority, the CNIL, suggests that employers can invite individual employees to share information about their own medical situation or potential exposure to the virus but directs companies not to deploy blanket medical questionnaires or introduce mandatory temperature checks.

Relatedly, the Irish Data Protection Commission’s COVID-19 [guidance](#) reminds companies to discharge their transparency obligations when collecting COVID-19–related data, including clearly communicating the purpose for which the data is collected and for how long it will be retained. Furthermore, any data collected must be safeguarded and disposed of appropriately; the German [guidance](#) reminds companies that data collected to help manage this crisis cannot be used for other unrelated purposes and should be deleted as soon as it is no longer needed.

Maintain Detailed Records of COVID-19–Related Data Processing Decisions and Impact. In line with the GDPR’s accountability principle and record keeping requirements (**Articles 5(2) and 30**), companies should record the decision-making process underlying COVID-19–related personal data measures and steps taken to ensure data protection compliance. This includes recording the lawful basis for processing the data; typically, either necessity for “reasons of public interest in the area of public health” (**Article 9(2)(i)**) or necessity for discharging “obligations in the field of employment” where local laws require companies to safeguard their employees (**Article 9(2)(b)**).

It seems likely that many companies will find it challenging to meet their data protection obligations - for example, responding to data subject access and other rights requests - due to staffing or technological issues caused by the pandemic. The ICO's [guidance](#) says it will not punish organizations that "need to prioritise other areas or adapt their approach during this extraordinary period." Considering the possibility that other supervisory authorities may be less forgiving, a best practice would be to carefully record the reasons for any delays or defaults, and contemporaneously to collect and maintain supporting evidence.



Jeremy Feigelson
Partner, New York
+1 212 909 6230
jfeigelson@debevoise.com



Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Jane Shvets
Partner, London
++44 20 7786 9163
jshvets@debevoise.com



Robert Maddox
Associate, London
+44 20 7786 5407
rmaddox@debevoise.com



Alexandre Bisch
Counsel, Paris
+33 1 40 73 13 37
abisch@debevoise.com



Ariane Fleuriot
Associate, Paris
+33 1 40 73 12 77
afleuriot@debevoise.com



Fanny Gauthier
Associate, Paris
+33 1 40 73 12 90
fgauthier@debevoise.com



Dr. Friedrich Popp
Associate, Frankfurt
+49 69 2097 5281
fpopp@debevoise.com