Katten

PRIVACY, DATA AND CYBERSECURITY ADVISORY

UK ICO Issues Guidance on COVID-19 Data Protection Considerations

March 27, 2020

The Information Commissioner's Office (ICO) has issued a statement confirming that data protection will not stop the need for businesses to share information quickly, or adapt the way they work to face the unprecedented challenges of COVID-19.

Similarly, the European Data Protection Board (EDPB) has confirmed that data protection rules (such as the GDPR) will not hinder the measures taken to fight against the pandemic. However, the EDPB does underline in its statement that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of data subjects.

This Katten Q&A sets out some points that organisations subject to the **GDPR/UK Data Protection Laws** may wish to consider when handling personal data in connection with their COVID-19 management and mitigation strategies.

Will I be penalised for delays in meeting Information Rights Requests?

No. In recognition of the diversion of resources (such as finances or people) from data protection compliance procedures that organisations may now need to make, the ICO has confirmed that (whilst not extending statutory timelines) it will not penalise businesses who do not meet the deadlines for responding to a data subject request of one month, or three months in complex cases.

Should there be any anticipated delays, it is recommended that you keep data subjects up to date on progress of the response.

What data can I collect in relation to COVID-19?

You have an obligation to protect your employees' health, but that does not necessarily mean you need to gather lots of information about them. You should only collect personal data that is necessary, and any information collected should be treated with the appropriate safeguards.

In the context of coronavirus containment, this means collecting only the information needed to 1) evaluate the risk that an individual carries the virus; and 2) take proportionate risk-based measures. Accordingly, the information collectable from employees could be:

- the presence of COVID-19 symptoms;
- confirmation of the individual's travel to a particular country; and
- indication of any close contact that the individual may have had with persons who may 1) have visited a particular country; or 2) be showing COVID-19 symptoms.

It is recommended that you ask visitors to consider government advice before they decide to attend, as well as advise staff to call 111 if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

How can I use data collected in relation to COVID-19?

Health data is special categories of personal data. To process this data quickly (which may mean without the consent of the data subject), you will need to identify the most appropriate condition under the GDPR. The EDPB notes that, from an employment context, processing of personal data may be necessary for compliance with a legal obligation to which you, as an employer, are subject to. This includes obligations relating to 1) health and safety at the workplace; or 2) the public interest (such as the control of diseases and other threats to health).

The EDPB also references the ability to process certain special categories of personal data where it is necessary for reasons of substantial public interest in the area of public health, on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject.

You must ensure that individuals whose personal data is collected receive a privacy notice that details how their data will be used.

Can I tell my staff that a colleague may have contracted COVID-19?

Yes. The ICO has advised that you should keep staff informed about cases in your organisation. However, the GDPR may not give you the right in all circumstances to name the individual, so if you do not need to name them, you should not do so, and you should not provide more information than necessary.

The EDPB adds that in cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g., in a preventative context), the concerned employees should be informed in advance and their dignity and integrity protected.

Considerations under the Data Protection Act 2018?

If you are a business subject to the Data Protection Act 2018 (DPA), when processing health information relating to COVID-19, in addition to meeting the requirements discussed above under the GDPR, you will need to identify a condition under Schedule 1 of the DPA for processing special categories of personal data. For example, if you are seeking to rely on your right to process personal data without consent under one of the permitted conditions set out in the GDPR, you also will need to put a policy document in place under the requirements of the DPA. This document must include the relevant condition(s) for processing the data, how your organization the data controller can satisfy a lawful basis for that processing, and specific details about applicable retention and deletion policies.

Homeworking during the coronavirus outbreak?

If it is necessary for staff working from home to use their own device or communications equipment, you may permit them to do so. The ICO guidance states that data protection laws will not prevent the use of personal devices, but you will need to consider the same kinds of security measures for homeworking that you would use in normal circumstances. Employers should carry out a data privacy risk assessment of the data protection implications of employees working from home on a scale greater than might be usual.

Whilst not an exhaustive list, you could ask staff to do the following:

- Avoid saving personal data to unsecured devices or cloud storage.
- Be on the lookout for phishing, hacking scams and the risk of cybercriminal activity.
- Create complex passwords that are changed often.
- Change default home Wi-Fi passwords and use only secure Wi-Fi networks.
- Delete files from download folders and trash bins.
- Immediately report lost or stolen devices.
- Install firewalls and anti-malware/anti-virus software on personal devices and ensure all operational software is kept updated.
- Avoid using ‘remember password’ settings on login pages.

- Do not share passwords with family members.
- Do not save documents locally on shared devices.

You may wish to update your security policy to inform staff of how they can ensure the continuing security of personal data whilst working remotely. For more information see our guidance on 'Cyberhygiene Dos and Don'ts for COVID-19 Remote Work'. [1] In addition, the National Cybersecurity Centre has issued some useful guidance to assist organisations in managing the increased cybersecurity challenges that could be consequent of increased home working.[2]

Final Thoughts

Ultimately, it is about adapting your data protection compliance procedures to factor in any additional steps and considerations that may be required to implement your coronavirus management strategies, whilst as the ICO states '*being proportionate and avoiding any measures that may be seen as excessive from the public's point of view*'.

---

[1] https://katten.com/coronavirus-cyberhygiene-dos-and-donts-for-covid-19-remote-work

[2] For additional remote working recommendations from the National Cybersecurity Centre see guidance at (https://www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19).

CONTACTS

For more information, contact your Katten lawyer or any of the following:

Christopher Hitchins
+44 (0) 20 7776 7663
christopher.hitchins@katten.co.uk

Shanthi Fallon
+44 (0) 20 7776 7642
shanthi.fallon@katten.co.uk

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@katten.com

Trisha Sircar
+1.212.940.8532
trisha.sircar@katten.com