COVID-19 ALERT:
IMPACTS ON CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT

MARCH 2020

By Barry Fishley and George Mole

To slow the spread of the current COVID-19 pandemic, governments across the world have been imposing stringent restrictions on people's movements. The prevailing message is to work from home if possible. Meanwhile national data protection authorities across Europe as well as the EDPB (the independent European body set up to promote compliance with European data protection laws), have published guidance discussing the impacts of COVID-19 on data privacy.

But what are the data privacy and cybersecurity risks associated with working from home, collecting health data and notifying staff of suspected cases of COVID-19 within the organisation, and what practical steps can organisations take to mitigate these risks?

Working from home

This poses threats to cybersecurity and data privacy from both an operational and a technical perspective. Operationally, working from home will mean that some staff will unavoidably be in the company of members of their household. Such staff will need to take extra care when taking telephone calls, working from (and disposing of) hard copy documents and leaving their computer unattended to ensure that they continue to protect confidential information and personal data.

Technically, staff may be at greater risk of cybersecurity vulnerabilities if they connect to unsecured Wi-Fi networks (which are common in coffee shops, if they are open!), or use personal devices which may have a lower level of security protection in place (e.g. a 4-digit passcode rather than an alpha-numeric password). It is also important to flag that bad actors are already taking advantage of the current climate of uncertainty by sending out an unprecedented amount of phishing (and, more targeted, spear-phishing) emails purporting to be from organisations like the World Health Organisation and HMRC. Organisations should take steps to ensure staff are implementing appropriate security standards at home, remind staff to be diligent when accessing external links (hovering over them to reveal the true web address before proceeding) and ask staff to implement measures in accordance with the organisation's policies on information security, privacy, confidentiality, remote working and the use of personal devices.

Collecting and monitoring health data

In the ICO's Guidance on COVID-19 (the "**Guidance**"), it stated that it is reasonable for organisations to ask staff to notify the organisation's HR team if they suspect they have contracted symptoms of, been diagnosed with, or are at an increased risk of contracting, COVID-19. Organisations need to ensure the health and safety of their staff and have a duty of care towards them and collecting such health data may be necessary to comply with these obligations. The Guidance does not, however, alter the statutory requirements on controllers of personal data to (a) provide fair processing information to data subjects when collecting their data; and (b) ensure the organisation has a lawful basis for processing such personal data.

Organisations should ensure that (a) their staff (and, if relevant, customer or visitor) privacy notices are updated to collect health data; (b) they only collect the personal data necessary (e.g. to fulfil its obligations to protect its workforce); and (c) record the lawful bases on which they rely to process health data.

Obligation on employees to disclose health information

There may be some misconception that the GDPR puts an obligation on employees to disclose their health data to employees. To be clear, there is no such obligation on data subjects under the GDPR. Therefore, in light of the COVID-19 pandemic, organisations will need to trust its employees to 'do the right thing' and self-isolate if they are at risk of contracting, or are showing symptoms of, COVID-19. If a staff member tries to 'soldier on', organisations should consider forcing that staff member to take sick leave.

Notifying other employees of suspected or diagnosed cases of COVID-19

Organisations may need to inform staff of suspected, or diagnosed, cases of COVID-19 in order to keep its staff healthy and safe. The fact still remains that no more personal data about an employee should be disclosed to other employees than is necessary and, often, it will not be necessary to disclose *any* personal data. If the identity of the suspected or diagnosed staff member does not need to be

COVID-19 ALERT:
IMPACTS ON CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT

MARCH 2020

> *Where organisations **need** to divert resources from data privacy compliance to other areas of its business to deal with the pandemic, those organisations will not be penalised. However, this does not alter the statutory obligations on... employers*

disclosed for the organisation to fulfil its obligations to keep its other staff members healthy and safe, then it should not be disclosed. If it does, then the disclosure should just be to a limited number of people, such as the immediate team with whom the employee works. In addition, the affected employee should be informed in advance of this disclosure.

The regulatory landscape and complying with statutory timescales

The Guidance states that the ICO recognises organisations have an obligation to ensure the health and safety of staff and a duty of care towards them – data protection does not prevent those obligations being fulfilled. It goes on to say that where organisations *need* to divert resources from data privacy compliance to other areas of its business to deal with the pandemic, those organisations will not be penalised.

However, this does not alter the statutory obligations on those employers to notify the ICO of data security breaches without undue delay (and, in certain circumstances, within 72 hours of becoming aware) and to respond to any data subject access request ("**DSAR**") within 1 month of receiving it. If an organisation receives a DSAR now, it should consider whether it has the capacity to fulfil the request within 1 month or whether it might need to notify the data subject that it will need more time.

Key takeaways

- Ensure staff members are aware of the increased risk of phishing emails and the operational and technical steps they should take while working remotely to ensure the security of confidential information and personal data.
- Organisations should only collect and disclose health information to the extent required to protect the health and safety of their workforce.
- The GDPR does not oblige employees to disclose health information to their employers, therefore organisations should ask staff to be honest about symptoms and self-isolate if necessary.
- Where organisations need to divert resources from their regular compliance function, the ICO will not penalise them. However, organisations should still be aware of statutory timelines for notifying the ICO of security breaches and responding to DSARs (and notifying data subjects of any extra time the organisation might need to comply with their request).

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
George Mole	View Bio	george.mole@weil.com	+44 20 7903 1367