Commercial & Tech Law Blog

Privacy and data security issues amidst the Coronavirus (COVID-19) pandemic

Posted on March 19, 2020April 4, 2020 by eyadmin

Alex Razak
(https://web.archive.org/web/20200720221118/http://www.linkedin.com/in/zxr) |
Manager | Law | +447341079034 | alex.razak@uk.ey.com
(https://web.archive.org/web/20200720221118/mailto:alex.razak@uk.ey.com)

Background

As COVID-19 continues to spread and increased restrictions are put in place, more and more people will be working from alternative locations and organisations will be taking measures to protect their staff.

In this note, we highlight key privacy and information security issues that businesses should consider as part of their business continuity measures as well as when taking steps to fulfil their duty of care towards employees. The issues are also relevant to other stakeholders including contractors and visitors.

This note is not intended to provide an exhaustive list of issues. Nor should it be relied upon as legal advice. Please do contact us if you require legal advice on any specific issues.

Can we collect information about health and recent travel?

Organisations may collect information on symptoms, recent travel and exposure to affected individuals. Organisations would need to comply with the data processing principles under the GDPR, including principles relating to lawfulness, fairness and transparency as well as security and confidentiality. The conditions that apply to the collection and processing of special categories of personal data also apply when collecting health data. Key considerations are set out below.

- **Conduct a data protection impact assessment (DPIA).** The processing (including collection) of data concerning health (including information regarding symptoms and medical conditions) on a large scale necessitates a DPIA being carried out prior to the processing taking place. Furthermore, organisations must carry out a DPIA for processing that is likely to result in a high risk to individuals. Most organisations will be required to carry out a DPIA.

- **Identify the lawful basis for processing.** The lawful basis for processing personal data

should be identified on a case-by-case basis. Appropriate bases include "legal obligation" (the legal obligation must be laid down in UK or EU law and can include common law obligations such as duty of care) or "vital interests".

- **Identify the conditions for processing health data (including symptoms).** Processing of personal data concerning health such as information regarding symptoms requires additional conditions to be met because health data is a special category. Organisations may rely on conditions which recognise that processing is necessary under UK or EU law in the field of employment (health and safety) or public health (protecting against serious cross-border threats to health). Explicit consent is unlikely to be available for general application.

How can we collect the information?

Whilst this would require a case-by-case assessment of an organisation's specific circumstances, an initial questionnaire to all members of staff or visitors could be appropriate as a first step.

- **Provision of information.** Organisations should provide individuals with information about the processing, as required under the GDPR. This information could be provided by way of a privacy notice prior to or at the time of data collection. The notice should contain information necessary to ensure fair and transparent processing, including the purposes of processing, the legal basis for processing and the recipients of data.

- **Ensure data minimisation.** Whilst compliance with all data processing principles is important, including security and confidentiality, it is imperative to ensure that any information that is collected (e.g. from staff or visitors) is adequate, relevant and limited to what is necessary. Information such as the individual's nationality or details of countries visited prior to the COVID-19 outbreak is unlikely to be considered necessary. Carefully drafted screening questionnaires for members of staff or visitors should assist in data minimisation. As per the ICO's guidance, visitors could be asked to consider government advice in advance of a visit. Staff could be advised to call the NHS helpline if they are experiencing symptoms or have visited particular countries.

- **Security and confidentiality.** Organisations would need to consider issues regarding security and storage of completed questionnaires.

Can we share information with other organisations and other members of staff?

Organisations can share information with third parties provided that the information sharing is in compliance with the GDPR and the Data Protection Act 2018. This will include a consideration of the issues listed above (e.g. consider a DPIA, identify lawful basis and conditions for processing special categories, provision of information to individuals, data minimisation as well as confidentiality and security). The ICO has stated that organisations should keep staff informed about cases of COVID-19 in the organisation but they probably do not need to name the individuals and should not provide more information than is necessary.

Has the ICO given guidance on the topic?

On 12 March 2020, the ICO released a statement (https://web.archive.org/web/20200720221118/https://ico.org.uk/for-organisations/data-

protection-and-coronavirus/) for organisations seeking to comply with their obligations under data protection and electronic communication laws in the UK in light of the current health emergency. Key takeaways are set out below.

- The ICO recognises that resources might be diverted away from compliance or information governance work. The ICO will not penalise organisations that need to prioritise other areas or adapt their usual approach. Statutory timescales will not be extended. However, the ICO will inform people through their own communications channels that they may experience delays when making information rights requests during the pandemic. This statement should give some comfort to organisations currently receiving requests from data subjects seeking to exercise their rights under the GDPR but who have to divert resources away in light of the current emergency.

- Data protection and electronic communication laws do not prevent the Government, the NHS or any other health professionals from sending public health messages to people, either by phone, text or email. These messages are not direct marketing and therefore prior consent of individuals is not required.

- Organisations and staff working from home should consider the same kinds of security measures for homeworking that would be used in normal circumstances.

- Organisations should keep staff informed about cases of COVID-19 in the organisation but they probably do not need to name the individuals and should not provide more information than is necessary.

- Organisations seeking to collect health data in relation to COVID-19 about employees or visitors or ahead of a conference or an event should not gather more information than is necessary. Visitors could be asked to consider government advice in advance of a visit. Staff could be advised to call the NHS helpline if they are experiencing symptoms or have visited particular countries. It is reasonable to ask people if they have visited a particular country or are experiencing COVID-19 symptoms. Any information collected should be subject to appropriate safeguards.

- Organisations can share employees' health information to authorities for public health purposes. However, the ICO states that it is unlikely that organisations will have to share information with authorities about specific individuals. We recommend that you seek legal advice before sharing employee health information.

Should we introduce enhanced security measures?

We are aware that there has been a spike in suspicious email messages attempting to take advantage of the COVID-19 emergency. Criminals are targeting individuals as well as industries, including aerospace, transport, manufacturing, hospitality, healthcare and insurance. It is a timely reminder for individuals and organisations to gear-up their cybersecurity awareness. Staff should be reminded of the organisation's information security guidelines as well as good practice guidelines on working remotely or from alternative locations, including using secure devices and secure networks. As a minimum, we would expect staff to carry out the steps set out below.

- Verify the sender by checking the email address.

- Check the link carefully before you click on it. Do not click on a link that you cannot recognise.
- Be careful when providing personal information and do not rush or feel under pressure. Cyber criminals use emergencies to get people to make decisions quickly.
- Report a scam or anything suspicious.

Can we be liable for breach of applicable laws?

COVID-19 is a global emergency affecting almost all aspects of life and day-to-day affairs of organisations. However, COVID-19 does not suspend an organisation's compliance obligations in relation to laws applicable to the processing of personal data and privacy as well as good information security standards.

How we can help

This note sets out some of the key privacy and information security issues that have arisen under England and Wales. These issues are also likely be arising in other jurisdictions. The issues caused by COVID-19 are not limited to privacy and information security – organisations should ensure that they comply with all applicable laws of the jurisdictions that they operate in. If you have any questions in relation to this note, please do get in touch with us.

Alex Razak

15.03.2020

Posted in Cyber Security, Data Privacy, GDPR, Online Communications