COVID-19 Data Protection and Cyber Security Issues to Consider

The ongoing COVID-19 pandemic has introduced a host of new data protection and cyber security risks. We explore below some of the most topical cyber and data protection issues for organisations to consider.

Processing of Health Data

The European Data Protection Board ("**EDPB**") adopted **a statement** and the Irish Data Protection Commission ("**IDPC**") released a **guidance note** on data protection issues to consider on the processing of personal data in the context of COVID-19. The key themes coming from both of these documents are relatively clear – data protection laws do not stand in the way of an effective response to COVID-19 but controllers should still be mindful of their statutory obligations.

In particular, organisations should be ensure that:

- they have an appropriate lawful basis for processing special category personal data (ie medical data);
- employees or other data subjects are fully informed and aware of any such processing activities; and
- any new processing practices (such as monitoring employees activity while they work from home) are carried out according to applicable laws.

Organisations should also ensure they document any decision-making process regarding measures implemented to manage COVID-19, which involve the processing of personal data. It would be prudent for organisations to keep a record of any public or governmental announcements supporting any decisions taken.

Planning for Data Breaches

Personnel who are working remotely will largely be doing so on company-issued devices, such as work phones, laptops and printers. This can lead to an increased risk of those devices being lost, misplaced or stolen. It is important to avoid a situation where sensitive company data accidentally ends up in the hands of third parties. Indeed, this is one of the most common forms of personal data breach notified to the IDPC each year.

COVID-19 presents two challenges in relation to data breaches. The first is that changing working environments may increase the likelihood of breaches happening. The second challenge is that the team who would normally deal with the response to a breach may not be readily accessible or may not have prepared to manage a large breach incident remotely.

Companies should ensure therefore that all mobile devices are properly encrypted and can be "wiped" remotely in the event the device becomes lost or stolen. These and other measures, which lower the risk of inadvertent disclosure of personal data, may help companies avoid notifiable data breaches.

Now would be a good time to update your data breach response plan to anticipate any new challenges that may be caused by more people working via remote access. Consider reminding staff of their obligations and of what policies apply. It is also vitally important that all employees are clear on who they should contact if they think there has been a personal data breach.

Dealing with Data Subject Right Requests

Data subject right requests will continue to arrive during the period when many organisations are working remotely. The IDPC address this specifically in a recent guidance note (**here**). The timelines for response to data subject right requests are set down in the GDPR and cannot be voluntarily waived by the IDPC (or any supervisory authority). However, the prevailing working conditions are likely (in some cases at least) to be a valid justification for seeking an extension on the deadline for response (as anticipated in Art. 12(3) GDPR).

The DPC goes on to note that:

- where a response to a data subject access request may be delayed, open and proactive communication with the data subject is important;
- organisations should consider responding to data subject access requests in phases (ie electronic files might be provided initially with hard copy files to follow when people have better access to their offices); and
- where a deadline is missed, and a complaint is made to the DPC, "the facts of each case including any organisation specific extenuating circumstances will be fully taken into account".

If you think you will miss a deadline then record the facts that have impacted on that failure, as you may need to explain how the current crisis has impacted on your ability to respond.

Security Challenges of Remote Work

New work environments can lead to new challenges. For example, some employees may find themselves sharing common living spaces with roommates or family members, when engaging in their work activities. This will undoubtedly pose a challenge to the confidentiality obligations that organisations may be under in the course of their day to day duties. Employees should be encouraged to engage in sensitive work practices, such as client calls, in private spaces and to not share work related information with individuals not employed in the same company or other third parties.

Helpfully, the DPC has issued some recent guidance on working remotely (**here**) which may be of assistance.

There can be a temptation to electronically store information locally on personal devices, rather than using standard company approved systems. Company staff members should be reminded not to store information in non-approved folders or systems. Employees should adhere to their company's data retention policies and be reminded that information should not be stored for longer than is necessary.

Many personnel will want to print hard copy materials at home or bring hard copy folders home with them to use for work purposes. This can lead to a greater risk that such information will be lost or misplaced. Additionally, it is common for personnel not to engage in proper data disposal methods (such as paper shredding) when working from home. Companies should endeavour to warn their personnel of these potential dangers and to encourage them to use only necessary hard copy materials, to dispose or return such materials correctly, and to operate at all times in line with the company's IT security policies.

Now is also a good time to review and update any policies covering agile working, acceptable use of IT equipment, cyber security, or BYOD. Employee-facing data protection notices may also need to be updated or supplemented to meet the changing ways in which personal data may be processed.

Malicious cyber security campaigns targeting remote workers

'Bad actors' unfortunately are not slow to take advantage of new potential vulnerabilities. Phishing and other cyber-attacks have increased as businesses and individuals deal with the challenges posed by COVID-19. For example, there has been an increase in fraudulent "phishing" emails sent by criminals impersonating organisations such as the World Health Organisation. A standard example of such an email is where the recipient receives an infected attachment with a fictitious title, such as 'COVID-19 safety protocols'. We expect potential threats of this nature to increase as businesses and individuals adjust to decentralised working environments.

Companies should continue to work closely with their internal IT and business continuity teams in order to identify any potential security gaps or additional cyber risks that may arise due to changing work practices.

Conclusion

The business landscape is being transformed by our response to the COVID-19 pandemic. It is important to strike a balance between taking the steps necessary to continue functioning and observing obligations in relation to the processing of personal data. Cyber security risk has probably increased in the last number of weeks and organisations should continue to be vigilant in this regard. Consistent and effective communication with customers and personnel is key to managing data protection and cyber risk.

Summary: In this short note we address the most common data protection and cyber risk issues that we have seen since the outbreak of the COVID-19 pandemic. The new business landscape brings additional data protection and cyber risk. Clear policies and thoughtful implementation will go a long way to addressing this risk.

For more information, please contact Chris Bollard, Deirdre Kilroy or Anne-Marie Bohan or your usual Matheson contact.