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 ("COVID-19 Data Protection and Cyber Security Issues to Consider") in relation to the processing of personal data in the context of COVID-19. The key themes that arise 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 still need to be mindful of their obligations.

In particular, organisations should be ensured that:

- they have an appropriate basis for the processing special category personal data (e.g. 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 be likely doing so on company-provided devices, such as work laptops, laptops and printers. This can lead to an increased risk of those devices being lost, misappropriated or stolen. It is important to avoid situations where sensitive company data accidentally winds 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 the changing working environments may increase the likelihood of data breach situations. The second is that the changing environment may increase as businesses and individuals adjust to decentralised working environments.

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 inappropriate disclosure of personal data, may help companies avoid certain data breaches.

Now would be a good time to update your data breach response plans to anticipate any new challenges that may be caused by more people working with remote access to company information. Preparing and training your employees and IT staff about your data protection policies and procedures may help them understand how to protect company data.

Dealing with Data Subject Right Requests

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

The EDPB guidance notes 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 (e.g. electronic files might be provided first with hard copy documents to follow when people have better access to their offices); and
- where a deadline is missed, and a complaint is made to the EDPB, "the facts of each case including any organisation's specific operating circumstances will be fully taken into account".

If you think you may need to deal with a raised threshold of the facts that have impacted on that failure, you may need to explain how the current crisis has impacted on your ability to respond.

Security Challenges of Remote Work

New environments can lead to new challenges. For example, some employees may find themselves sharing living spaces with non-workmates or family members, when engaging in their work activities. This will undoubtedly pose a challenge to the confidentiality obligations that organisations have to their employees. It is important that the data controllers/processors encourage members of the workforce, e.g. employees, to act in such a way that it is unlikely that personal data is accessed by people other than those who are entitled to access it. In particular, organisations should be ensure that:

- 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.

Helpfully, the EDPB has issued some recent guidance on working remotely. Here may be of assistance.

There can be a temptation to electronically store information locally on personal devices, rather than using standard company approved data disposal methods. This can lead to an increased risk that such information will be lost or misplaced. 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 Data Protection and Cyber Security Issues to Consider

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

For more information, please contact Data.Breaches@matheson.com or one of our Matheson COVID-19 experts.