BEALE&CO

CORPORATE & COMMERCIAL

COVID-19: Data Protection Issues

Authors:
Niamh Loughran
Sean O'Halloran

Date:
April 2020

Across the world, governments have introduced stringent regulations to limit the spread of coronavirus. The UK and Ireland have seen some of the strictest rules, with employees generally prevented from travelling to work, except in certain essential sectors. Countless organisations have adapted to the situation by allowing their employees to work remotely, either by expanding the use of their existing IT infrastructure to provide all employees with access to their systems, or by quickly adopting new systems and technologies to facilitate employees working from home.

Many of these changes will have data protection implications. New means of accessing data in new locations exposes it to greater risk. Furthermore, remote working increases the probability that an organisation will not be able to identify a data breach, particularly if employees use personal devices to access, store or share data. Employees using their personal devices to carry out work, or using personal work equipment at home, particularly for lengthy periods of time, also creates an inevitable blurring between home and work life.

Finally, employers must be conscious of their employees' own rights as data subjects. Questions such as whether an employer may share an employee's personal health information with employees (such as the fact that a team member or their family has been diagnosed with COVID-19) will have data protection implications.

Background

The General Data Protection Regulation (GDPR) and Data Protection Acts require data controllers and data processors to implement technical and organisational measures that ensure a level of data security that is appropriate for the level of risk presented by processing that personal data. In order to achieve this, data protection laws impose a requirement of data protection by design and by default.

In addition to requiring data security, data protection laws also create many rights for data subjects. The most well-known of these being the right to make a subject access request.

Data Protection Begins at Home

Employers are responsible for taking the appropriate measures to ensure the protection of data used and processed by employees working remotely. There is nothing preventing employees using their personal devices for work purposes, but allowing them to do so generates obvious data protection risks.

The following are some practical tips employers can implement to ensure compliance with data protection laws for employees working remotely during COVID-19:

- Draft a framework specifying the appropriate technical and organisational measures which need to be implemented to ensure that personal data is kept confidential
- Log the devices and apps employees are using to store and exchange data
- Ensure that employees' devices are password protected, encrypted, and can be wiped remotely
- Remind employees to not use personal email addresses for work purposes

- Arrange ongoing training for employees to remind them of their data protection obligations
- Record in a single register details of all paper records and files that employees bring home from the office

Employees should be reminded that telephone conversations and video conference calls create the risk of being overheard. Employees must ensure that they are not discussing customer or other personal data where family, flatmates, or neighbours can eavesdrop. Similarly, virtual assistants in employees' homes are always "listening" and could be accidentally triggered to store the contents of a telephone conversation on their servers. Such devices are also vulnerable to being hacked and employees should be advised to turn these devices off when working at home.

New Systems: New Risks

Cloud storage offers one of the best means to ensure that data is held securely whilst also being accessible to employees wherever they are. Cloud storage is not without risks, however. The following are some practical steps an organisation can take to reduce the risks associated with cloud storage:

- Review any existing data protection agreements with customers to ensure cloud storage is permissible
- Choose a reputable company whose servers are based in the European Economic Area[1] or other country that meets adequate data protection standards[2]
- Check the storage provider's terms and conditions and privacy notice
- Ensure that privacy settings are appropriate

Video conferencing apps and programs are increasingly easy to install and many offer a free of charge means for employees to communicate. However, many do not use unencrypted software. Organisations should ensure that any software their employees are using is encrypted and that privacy settings are in place to ensure work video conferences are not accessible by third parties.

Identify and Report Data Breaches as they Occur

The requirement to notify the authorities[3] in cases of data breaches is very strict. Where feasible, an organisation must report a breach no later than 72 hours after becoming aware of same. Furthermore, if there is a high risk that a breach may adversely affect data subjects they must be informed immediately. These time limits are unlikely to be affected by the current pandemic.

Whilst employees are working at home it will be more difficult for organisations to detect and respond to data breaches. Practical steps for employers to deal with these issues are as follows:

- Provide training to employees to ensure that they recognise a data breach
- Adopting a "no blame" culture with employees to ensure that they immediately notify management of data breaches and do not attempt a "cover-up"
- Documenting all breaches, even where the breaches do not need to be reported to the relevant government office, so your organisation can learn from these experiences

Data Subject Access Requests

Organisations are required to respond to data subject access requests in full or in part within one month of receiving same. This one month limit can only be extended where it is particularly complex. Where doing so, the organisation must let the requesting party know within one month of receiving their request that they will require more time, and explain the reasons why the extension is required.

If statutory timelines cannot be met owing to the COVID-19 pandemic, the data protection authorities in Britain and Ireland have confirmed that they will consider these

[1] European Economic Area consisting of the EU countries (plus the United Kingdom), Iceland, Lichtenstein, Norway.
[2] As of April 2020 these are Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States (limited to the Privacy Shield Framework only).

[3] In the United Kingdom the relevant statutory authority is the Information Commissioner's Office. In Ireland it is the Data Protection Commission.

complaints in the context of the time the requests were made to the organisation.

Employees' Rights: Monitoring

Organisations must be mindful that they are a data controller in respect to their employees, and must ensure that their employees' data protection rights are safeguarded. However, as lockdowns are extended, and employees work from home for long periods, employees will inevitably fail to differentiate between work time and personal time, creating a risk of them using work devices for personal use and vice versa. This can result in employees' personal data being stored on work devices and vice versa. Organisations should remind employees to avoid this where possible.

Noting that it may be difficult for employers to monitor their staff, many organisations have, or are considering the installation of software that monitors internet usage, logs keystrokes, records screens, etc. These systems offer an attractive means to ensure that productivity remains high. However, monitoring systems create privacy concerns. Organisations considering the use of new monitoring systems should only do so following the completion of a full Data Protection Impact Assessment that weighs the rights of employees against the need to ensure productivity on the part of the organisation. If such systems are already in use, employers should refresh existing policies and recirculate them to employees to explain when and how they are being monitored, and the reasons they are being monitored.

Employees' Rights: Infected Employees

Discovering that an employee has been diagnosed with COVID-19 will create issues for organisations, particularly where an infected employee has come into physical contact with other staff. Employers will be required to balance their duty of care to the employee's colleagues with that employee's privacy rights, particularly as data protection law creates stricter safeguards for sensitive personal data, such as health information.

If an employee informs an employer that they or a family member have been diagnosed with COVID-19, the employer may be able to rely on one or more of the following legal basis to disclose this fact to their colleagues:

- Compliance with a legal obligation that an employer is subject to
- Vital interest (where life is at risk)

It is important that the employer clearly explains to the infected employee that they are notifying only those colleagues who they may have come into physical contact with. They should also explain to the affected employee that they are doing so in compliance with the employer's obligation to protect other staff members. Finally, to the extent that it is possible, the organisation should avoid naming the individual infected.

Conclusion

There are a number of data protection considerations that organisations must constantly consider in response to the COVID-19 pandemic, particularly as new IT systems are rapidly introduced.

By having regard to essential privacy principles, and ensuring that existing policies are updated accordingly, organisations can ensure that they safeguard the rights of data subjects during the pandemic, while at the same time maintaining productivity.

This article aims to provide some practical tips to implement within your organisation but specific legal advice is always recommended.

For further information please contact:

Niamh Loughran
Partner
+353 (0) 1 536 9614
n.loughran@beale-law.com

Sean O'Halloran
Solicitor
+353 (0) 1 536 9621
s.ohalloran@beale-law.com