TECHNOLOGY

Data Protection and COVID-19: Topical Issues and What You Need to Know

9 April 2020

With a constant stream of guidance and advice, we have set out some of the main issues at the intersection of data protection and COVID-19 in Ireland.

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Ciara Anderson
Associate
+1 415 829 4247
Ciara.Anderson@arthurcox.com

Caoimhe Stafford
Associate
+353 1 920 1328
Caoimhe.Stafford@arthurcox.com

It is important to keep in mind, as the Data Protection Commission ("**DPC**") has said, "*[d]ata protection law does not stand in the way of the provision of healthcare and the management of public health issues*", as we all take the necessary steps to contain the spread and mitigate the effects of COVID-19.

WORKING FROM HOME

With most workers at home, the DPC has produced helpful guidance on remote working and guidance specifically on video conferencing. Some tips include ensuring work devices are updated regularly with regard to both the operating system and any software upgrades/patches. If available, the use of multi-factor authentication is always recommended. Where possible, video conferencing systems should be accessed through a secure virtual private network ("**VPN**") to protect against unauthorised access. Where it is necessary to save documents locally these documents should be backed up on the company's secure system as soon as possible and deleted from local drives. Extra care should also be taken of paper records in a home environment as these must still be kept in a secure manner and confidentially destroyed when no longer needed.

ILL EMPLOYEES

Some of the most pressing data protection issues have arisen in the employment context. For example, if an employer is notified by an employee that they have tested positive for COVID-19, the DPC has made clear in its guidance that disclosure of this employee's name to their colleagues should be avoided in the interest of maintaining confidentiality. Instead, an employer may inform staff that there has been a (suspected) case without naming the individual. In certain situations, an employer may be justified in disclosing the name and health status of an employee who has contracted COVID-19 if this employee was in close contact with members of their team.

Arthur Cox has also published a COVID-19 Employment FAQ article, which discusses the data protection issues and other employment implications of COVID-19, which may provide a helpful overview.

TEMPERATURE CHECKING

We are aware a number of organisations that have considered, or are already engaging in, temperature checking of staff, particularly in the medical device/ pharmaceutical manufacturing and food production sectors. Regardless of the sector, the employer must ensure it has a lawful basis for such checks and processing of the subsequent health data, meaning that it must be able to identify a legal basis under Article 6 of the GDPR, and an exemption under Article 9 of the GDPR. Since this is a novel type of processing for most organisations involving sensitive employee health

data, we also suggest conducting a data protection impact assessment to set out the probable risks to staff privacy rights and the safeguards in place to mitigate these risks.

ENSURING LAWFUL, FAIR AND TRANSPARENT PROCESSING

Organisations gathering additional health data on visitors and/or staff should always ensure they have a valid lawful basis for processing under the GDPR and the Data Protection Act 2018 ("**DPA**"). Where organisations are acting on the guidance or directions of public health authorities or other relevant authorities, Article 9(2)(i) of the GDPR and Section 53 of the DPA may permit the processing of personal data, including health data. However, suitable safeguards must also be implemented, such as pseudonymisation, restrictions on access to the data, strict time limits for deletion and appropriate staff training.

Employers also have a legal obligation to protect their employees under the Safety, Health and Welfare at Work Act 2005. In this case, an employer may rely on Article 9(2)(b) of the GDPR and Section 46 of the DPA as a legal basis to process personal data, including health data, for health and safety purposes. As with most lawful bases, the organisation should always consider and document why the processing is necessary for, and how the processing is proportionate to, the ultimate purpose.

Staff and visitors should be fully informed of any new type of processing either by physical notice on entry, email notification or an update and circulation of an existing privacy notice.

Organisations should also be careful that they do not use existing data sets for new purposes if this purpose is not compatible with the original purpose for processing. For example, DPC guidance on CCTV suggests that retaining CCTV footage indefinitely "just in case" an employee lodges a claim beyond the organisation's usual retention period (generally 30 days) would not be considered proportionate processing.

DSARS

The DPC has also released helpful guidance on data subject access requests in light of COVID-19. While this guidance confirms that the law (and the statutory time periods for response) has not changed, the DPC does recognise "*that unavoidable delays may arise as a direct result of the impacts of COVID-19*". In such circumstances, communication is key.

Mindful of stretched resources, it may be helpful to ask the requestor to narrow the scope of their request or choose to provide records in stages. If personal data contained in hard copy records are not currently accessible, this should be communicated to the individual and copies of these records should be provided when premises can be safely accessed.

If an organisation is not in a position to respond to a request within the statutory timeframe, it should (a) notify the individual as soon as possible and (b) keep a record of this communication and the reasons for the delay in order to meet its accountability requirements under the GDPR. If circumstances and timeframes change, the individual should be kept up-to-date.

We discuss this issue further and the position under the Freedom of Information Act 2014 in this article.