Workplace video surveillance (2) (3/39/19)

This article completes what we wrote last week.

Duty of notification

Video surveillance on a company's premises means that the employer is processing the personal data of current, former and prospective employees as well as customers and vendors.

In addition to informing data subjects about video surveillance in its privacy information and internal policies, the company should put up signs in front of any entrance to its video surveillance area giving at least the following information:

- a notice saying that video surveillance equipment has been installed;
- the full name, address and other contact details of the data controller (person in charge); and
- the purpose of video surveillance.

A company that installs video surveillance equipment to safeguard its property must respect the right of visitors and passers-by to privacy and protection of their personal data.

In its ruling C-212/13 of 11 December 2014, the CJEU stated that where an individual has installed video surveillance cameras on their property to safeguard property, health and life but this system also monitors a public area, this is not considered by law to be data processing only for private or domestic purposes.

So the company may do video surveillance on its property, but no video surveillance is allowed outside its property, i.e. surveillance records showing any adjacent property and private or public roads. Likewise, any video surveillance done to safeguard company vehicles parked outside its property is illegal.

A company doing video surveillance outside its premises should seek approval from the National Data Office or the municipality.

We recommend making sure that signs are put up at all entrances to the company's premises and that those signs and the company's privacy statement give sufficient information to meet GDPR requirements.

Storage periods

Data storage periods should be based on the purpose of data processing and kept to the statutory minimum. It is advisable to store data for only a few days before doing necessary reviews of the incident and using the recordings to bring a disciplinary or an administrative action, or a criminal prosecution.

After the purpose of data processing no longer justifies it being stored in an active database, it should be deleted, anonymised or archived in a separate database unless its storage is necessary for performing legal obligations or important for future litigation, always provided the storage period remains limited to what is absolutely necessary.

Key takeaways

Video surveillance breaches are among the most common data protection breaches. This year the National Data Office has imposed penalties in more than 40 cases, including breaches arising from video surveillance of residents over a wide area and/or data used for any purpose other than to safeguard property.

PwC Legal conducts data processing reviews for compliance with GDPR requirements, makes recommendations on data protection matters, develops various internal policies and procedures, runs training courses for corporate employees, and offers data protection expert services.