What should businesses know about video surveillance? (1) 1/31/23

Video surveillance may be treated as personal data processing by automated means if particular persons can be recognised in the footage. We often get asked if security cameras may be installed if they cover only an area, if nobody can be recognised in the footage, if the footage is not retained, etc. The scope of the General Data Protection Regulation (GDPR) excludes any personal data processing someone merely does as part of a private or domestic event.[1] This article takes a brief look at steps you should take to ensure your video surveillance is lawful.

The need to set up video surveillance

Before installing a security camera, you need to determine the purpose of data processing. This may have multiple purposes and each of those must be valid. This also applies to two or more security cameras if each has its own purpose of processing. The most common purpose of video surveillance is to protect a person's life, health and property, and to detect damage.

Before installing security cameras, the controller should check for any alternative measures he could take instead of video surveillance. If this is set up to safeguard property, then it's advisable to document any prior incidents that caused the controller to put up security cameras. In certain cases there is a high risk of danger and a legitimate interest for video surveillance, e.g. in banks, shops selling valuable goods, and areas where crimes against property take place frequently.

The European Data Protection Board suggests evaluating the following alternatives to video surveillance:

- Fencing the property
- Hiring a security officer or officers
- Installing security locks
- Setting up a dummy camera[2]

The legal basis for video surveillance

The most common legal basis for video surveillance is a legitimate interest under GDPR article 6(1)(f). If video surveillance is based on such a legitimate interest, this should be clearly defined and the controller should run a balancing test for this data processing. The test should take account of the idea that a data subject's rights are more important than the controller's interests. Careful documentation is therefore needed to show why the controller's legitimate interest applies and how far it can affect the rights and interests of data subjects.

Video surveillance may also be legally based on any of the other conditions listed in GDPR article 6, such as consent where personal data processing is restricted to particular data subjects.

Technical measures during video surveillance

The controller should check that the cameras are secure by taking a number of technical measures, for instance:

- Physical security – safeguarding the system against theft, vandalism, natural disasters and accidental damage.
- System security – protecting the entire system, including the camera, electricity supply and other things related to infrastructure.
- Access control – only authorised personnel can access the system, its data and the room where security camera footage is analysed.
- Data accessibility – the data can be accessed only when necessary.

(to be completed in next week's Flash News)

---

[1] The National Data Office's recommendations for installing security cameras and performing video surveillance on an individual's private property, page 4

[2] The European Data Protection Board guidelines 3/2019 on personal data processing using smart devices, page 10