EDPB: Data Protection Guidelines on Video Surveillance

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

At its 17th plenary meeting on 28/29 January 2020, the European Data Protection Board (EDPB) adopted guidelines on the processing of personal data through video devices. The guidelines take into account a prior public consultation on the topic (see eucrim 2/2019, p. 105).

These guidelines examine how the GDPR applies in relation to the processing of personal data by video devices and how consistent application of the GDPR can be ensured in this regard. The examples are not exhaustive, but the general reasoning can be applied to all potential areas of use. They cover both traditional video devices and smart video devices.

The EDPB highlights that the intensive use of video devices has massive implications for data protection. It also affects citizens' behaviour. In particular, the technologies can limit the possibilities of anonymous movement and anonymous use of services. While individuals might be comfortable with video surveillance set up for a certain security purpose, for example, guarantees must be taken to avoid misuse for totally different and – for the data subject – unexpected purposes (e.g., marketing purpose, employee performance monitoring, etc.). The huge amount of video data generated, combined with new technical tools to exploit images, increase the risk of secondary use. Furthermore, video surveillance systems in many ways change the way professionals from both the private and public sector interact. The growing implementation of intelligent video analysis has contributed to high-performance video surveillance. These analysis techniques can be either more intrusive (e.g. complex biometric technologies) or less intrusive (e.g., simple counting algorithms). The data protection issues raised in each situation may differ, as will the legal analysis when one or the other of these technologies has been used.

In addition to privacy issues, there are also risks related to the possible malfunctioning of these devices and the biases they may produce. According to the guidelines report, research studies found that software used for facial identification, recognition, and analysis performs differently based on the age, gender, and ethnicity of the person, and algorithms are based on different demographics. Thus, bias is one of the major problems of video surveillance; data controllers must regularly assess the relevance of such identification methods and supervise the necessary guarantees. The EDPB ultimately stresses that "video surveillance is not by default a necessity when there are other means to achieve the underlying purpose."

The guidelines address the lawfulness of processing, including the processing of special categories of data, the applicability of the household exemption, and the disclosure of footage to third parties. Other analysed items include:

- Processing of special categories of data;

- Rights of the data subject;
- Transparency and information obligations;
- Storage periods and erasure obligations;
- Technical and organisational measures;
- Data protection impact assessment.

The EDPB – an assembly of the EEA data protection authorities and the European Data Protection Supervisor – works on consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities. (TW)

Corona Outbreak and Data Protection

The outbreak of COVID-19 and subsequent initiatives and policy measures have triggered many crucial privacy and data protection law issues. The VUB Law, Science and Technology Society Research Group has provided a collection of statements and materials on tracking initiatives and on European/international resources on the pandemic at its website.

In a statement of 19 March 2020, the European Data Protection Board (EDPB) provides an answer to several questions on data protection in the context of the fight against the COVID-19 pandemic. The statement focuses on the processing of personal data by both public health authorities and employers. The EDPB refers to EU data protection rules and stresses that the GDPR does not, in general, hinder restrictions of freedom in this emergency situation; however, these measures must be proportionate and limited to the emergency period. Under certain circumstances, the GDPR allows the processing of personal data in the interest of public health without the individual's consent. The EDPS statement also serves as a reminder of the core principles relating to the processing of personal data.

For the processing of electronic communication data, such as mobile location data, the e-Privacy Directive additionally applies. In this context, public authorities should first aim to process location data in anonymously (i.e., processing data should be aggregated in a way that individuals cannot be re-identified). This could enable the generation of reports on the concentration of mobile devices at a certain location ("cartography"). If it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the Member States to introduce legislative measures pursuing national security and public security. Such emergency legislation is possible under the condition that it constitutes a necessary, appropriate, and proportionate measure within a democratic society. If these measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals using electronic communication services the right to judicial remedy. The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union