GDPR Update - EDPB video surveillance guidelines

September 3, 2019

Introduction

In July 2019, The European Data Protection Board (EDPB) adopted draft Guidelines on processing personal data through video devices (the Guidelines). The Guidelines provide guidance on how to apply the EU General Data Protection Regulation (GDPR) in the event data is processed due to video surveillance. The Guidelines are currently open for consultation until 9 September 2019. The final version of the Guidelines is expected later this year.

The scope of the Guidelines encompasses the use of video devices that collect personal data. Video devices used to process personal data by EU competent authorities for the purposes of prevention, detection or prosecution of criminal offenses, or the execution of criminal penalties or for household purposes do not fall under the scope of the Guidelines.

The household exemption determines that purely personal or household activities are out of scope of the Guidelines. Video surveillance activities that process personal data in the course of the private or family life of individuals and is not made publicly accessible falls under the household exemption.

Legal basis

The Guidelines reiterate that a legal basis under GDPR must be determined in order for controllers to process personal data specifically related to video surveillance. However, the Guidelines highlight some subtle differences as to how a legal basis may be applied.

Firstly, video surveillance based on the mere purpose of “safety” is no longer sufficient or specific enough. The purpose of using video surveillance must be explicit and documented.

Secondly, controllers who claim to have a legitimate interest and necessity under Article 6 (1) (f) GDPR must (as always) consider whether their legitimate interest is compelling enough to override the interests and rights and freedoms of the data subject. The reasonable expectations of data subjects will play a role in this balancing test. For instance, it is reasonable for a data subject to not expect to be under surveillance in a sanitary facility, but it is reasonable for the data subject to expect to be under surveillance at an ATM machine or a bank.

Likewise, the video surveillance must be necessary. Consequently, other means (that are less intrusive) would not suffice. This includes the necessity of the video surveillance usage, but also storage of the data and what data is captured (i.e. are clips taken from the footage, faces blurred, etc.). The Guidelines stipulate that controllers must have taken (or at least considered) other measures before reverting to video surveillance. Examples the EDPB gives include fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better

lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls.

Thirdly, the EDPB Guidelines determine that there must be an existing issue to process personal data through video surveillance. Essentially, real life threats/situations will or may dictate whether video surveillance may be used by a controller. Not only will controllers have to specify the purposes for processing data under GDPR, but controllers will also have to make a case for processing personal data using video surveillance before any processing takes place (i.e. there have been previous robberies or presenting statistics on crime in or around the area).

Especially criteria one and two above are a clear step up from how at least the Dutch data protection authority (DPA) assessed video surveillance to date.

Lastly, consent is mentioned as a legal basis in the EDPB Guidelines, but this legal basis must be taken with a grain of salt and used in exceptional cases. It seems impossible to believe that controllers using video surveillance systems would collect the consent of data subjects in large areas before processing personal data. Therefore, consent as a legal basis would most likely be used in exceptional cases (e.g. individual monitoring of an athlete).

Disclosure to third parties

Any transfer or disclosure is considered as a separate processing activity and the controller would thus need a legal basis. Additionally, any footage that is disclosed to a third party, for instance law enforcement agencies, would then place a legal obligation onto the controller and would constitute as a new purpose. Where such disclosure is to law enforcement agencies, this is often done under a legal obligation. The new processing purpose is in such a case unproblematic. However, this may be different if the disclosure is not done pursuant to a legal obligation.

Moreover, aside from controllers determining a legal basis for the transfer, third party recipients must also determine their own legal analysis and identify their own legal basis for receiving and processing the material.

Processing special categories of data

Although video surveillance may collect special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, and data concerning health or a person’s sexual life or sexual orientation), this may not necessarily be the original purpose or intent. In such cases, the captured data would not qualify as special category data.

However, if data controllers wish to collect and process special categories of personal data they must identify an exception for processing special categories of data under Article 9 GDPR.

Video footage of an individual cannot, however, in itself be considered as biometric data under Article 9 GDPR if it has not been specifically and technically processed to contribute to the identification of an individual (i.e. for facial recognition). For it to be considered as processing of special category data it requires that biometric data (facial recognition) is processed “for the purpose of uniquely identifying a natural person”. To determine this, three criteria must be considered: 1) nature of data: data relating to physical, physiological or behavioral characteristics of a natural person; 2) means and way of processing: data “resulting from a specific technical processing”; and 3) purpose of processing: data must be used for the purpose to uniquely identify a natural person. Processing biometric data presents a problem if individuals have not consented to their biometric data being captured and are represented in the footage. Certain safeguards must be taken by controllers to ensure that data is stored safely and appropriately;, for instance controllers must consider appropriate places to store the data, retention periods, accessibility (including who may access), speech signals that indicate what data subjects are saying should not be identified.

Also, consent will not be valid if there is a clear imbalance between the data subject and the controller, as evidenced

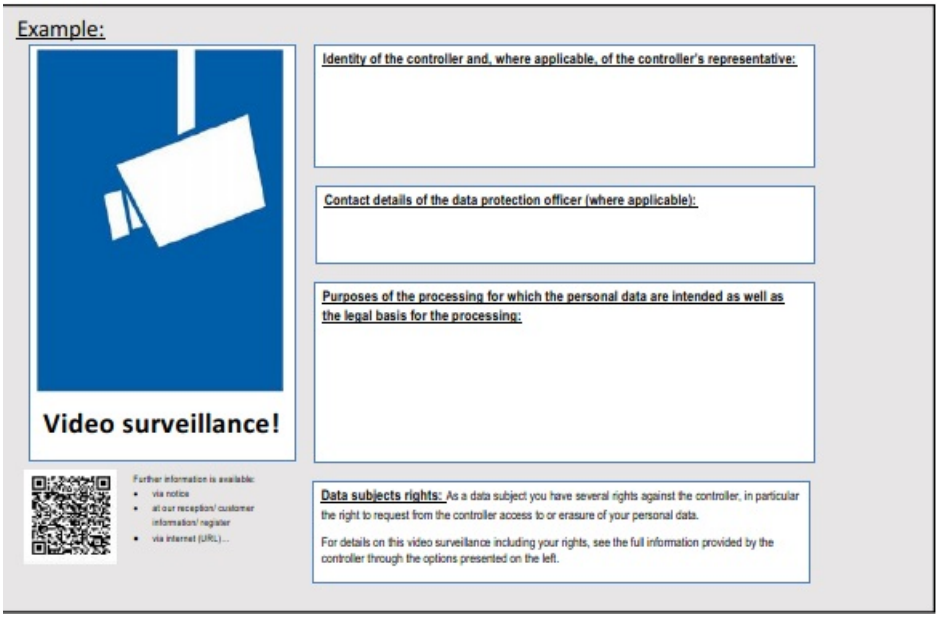
by a very recent fine (21 August 2019) issued by the Swedish DPA protection authority (Datainspektionen) against a school that used facial recognition to track students' attendance in school. This was done as a pilot in one class on the basis of consent, but the Swedish DPA ruled that this consent was invalid in view of the clear imbalance between the students and the school.

Rights of the data subject

The Guidelines further reiterate data subjects' rights under GDPR; however in terms of video surveillance these rights are more limited. Data subjects have the right to access, erasure and objection to the processing of their personal data. However, complying with these rights is not so straightforward. For instance, the right to access footage will be difficult as footage usually contains data of more than one individual, and if data subjects request to have access to such footage or copies controllers may not so readily comply. However, the Guidelines stipulate an interesting solution, where controllers may ask for more specifics regarding the data subject before searching for any footage (i.e. the timeframe). Moreover, the right to erasure does not necessarily mean that controllers will be able to erase data completely. Instead, blurring pictures or images as to not identify the data subject, and erasing the legal basis for processing will constitute erasure. Further, if any footage is published publicly then the controller has the obligation to take necessary steps to inform other controllers of the request. Objections can be made prior, during, or upon leaving surveillance areas. According to the EDPB, the right to object means that unless the controller has compelling legitimate grounds, monitoring an area where individuals could be identified is only lawful if the controller is able to immediately stop the camera from processing personal data, or if the monitored area is restricted so that the controller can ensure the approval from the data subject prior to entering the area. How this would play out in practice, the EDPB does not clarify. Our take is that whenever the video surveillance is for safety and security reasons (and this has been sufficiently clarified as per the comments above), the controller would typically have a compelling legal ground to continue the video surveillance.

Transparency

Data subjects should be aware that video surveillance is in operation, and the Guidelines identify two layers in which data subjects should be informed. The first layer is the most crucial as this is how the controller first engages with the data subject, thus warning signs must be displayed with an icon to give easily understood information of the processing taking place. Controllers may no longer display a sign that solely states, "You are under video surveillance". Instead, under the Guidelines the first layer must identify controllers, the purposes of the processing and data subjects' rights. Not only is the information regarding the processing of personal data more detailed, but it must also be strategically placed. According to the Guidelines, the warning sign must be positioned "at a reasonable distance" from the monitored area; that way data subjects are able to determine which area is under surveillance before they are captured (it is not necessary to divulge the precise location). The EDPB suggests the following sign:



The second layer requires that data subjects are also able to access any information regarding the video surveillance and the processing of data in hard copy and in the general vicinity of the area under surveillance. Digital sources are also permitted and must be mentioned in the first layer along with the QR code.

Here too, a number of practical issues arises. For example: how to deal with cameras located at the entrance of a store or shopping center? In such cases, it may not always be possible to provide the information before data subjects are captured. The Guidelines are – unfortunately – silent on this and other practical concerns.

Storage

The Guidelines determine the parameters of storing personal data accessed through video surveillance. The duration of storage of personal data may vary per Member States as they may have their own legislation on this matter, but the EDPB's default position is that camera footage should be deleted after one or two days. It is important to note that the longer data is stored the more the legitimacy of the purpose and necessity must be advocated. This is a clear deviation from the Dutch DPA's current practice, which allowed a standard retention period of four weeks.

Technical and organizational measures

Processing data should be both organized and secure, and data controllers have the obligation to ensure this. Additionally, controllers should select privacy-enhancing technologies for data protection by design and default functionality. Organizational measures must take into account the overall management and operation of the video surveillance system (i.e. who can access video surveillance, storage, who can monitor the video surveillance, measures for a data breach incident, maintenance, recovery procedures, etc.). Technical measures are vital to ensure that video surveillance systems are secure, meaning that systems should include data encryption features, firewalls or anti-virus detection systems, or even measures to physically protect the video surveillance system from theft, vandalism, or other accidents. Lastly, controllers will also need to pay special attention to access controls. For instance, ensuring that monitors are concealed, procedures for granting, changing, or revoking access are defined, user authentication methods are in place, etc.

Data Protection Impact Assessment

Under GDPR and further determined in the Guidelines, controllers are required to undertake Data Protection Impact Assessments (DPIA), particularly if the processing constitutes a systematic monitoring of publicly accessible areas on a large scale.

Given the data processed and the purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), many cases of video surveillance will require a DPIA. Therefore data controllers should carefully consult these documents to determine whether a DPIA is required.

Conclusion

When considering processing personal data through video devices, controllers and potential controllers should consider the following:

- Under which legal basis can I use video surveillance?
- Is there a real necessity to have video surveillance in place?
- Will I be processing special category data?
- How do I meet the transparency obligations, in particular the need to provide the first layer information before data subjects are captured by the cameras?
- How and how long will I store the footage, and is it necessary to store the footage at all?
- How will the video surveillance system be equipped to handle and protect personal data?
- Should I perform a Data Protection Impact Assessment?

Finally, the Guidelines are still in draft form and may be subject to changes. We advise to consult the final Guidelines before implementing any measures that have far-reaching practical or operational consequences. Of course, we will share a further update once the Guidelines are final.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability
July 2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)

December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in the Employment Context
April 2018	Profiling and Retail
May 2018	Overview
October 2018	Overview of developments since May 25, 2018
November 2018	Data Protection Impact Assessments (DPIAs)
December 2018	EDPB Guidelines on the territorial scope of the GDPR
February 2019	Camera Surveillance
May 2019	GDPR in the Netherlands: one year after
September 2019	EDPB Video Surveillance Guidelines

Dentons Boekel acknowledges and thanks Stefania Lessen for her contribution to the article.

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com