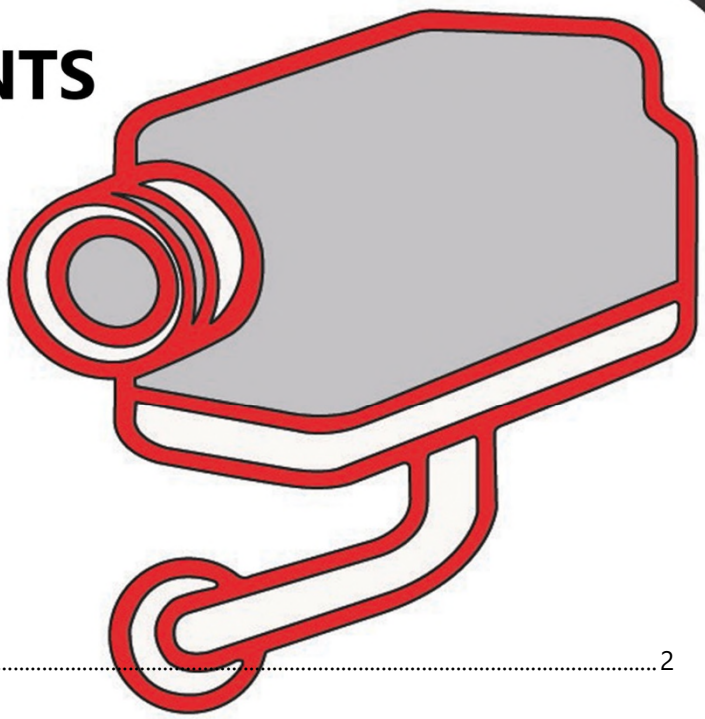
MAYER | BROWN

Legal Update

10 COMMANDMENTS

for Processing Personal Data Through Video Devices in the European Union



Data controllers/authors: Diletta De Cicco and Charles Helleputte
Address: Mayer Brown, Avenue des Arts 52, 1000 Brussels
Contact details: ddecicco@mayerbrown.com or chelleputte@mayerbrown.com

Introduction

On January 29, 2020, the European Data Protection Board ("EDPB") released Guidelines 3/2019 on processing personal data through video devices ("Guidelines"). The Guidelines shed light on the EU General Data Protection Regulation ("GDPR") requirements applicable to this type of processing.

While some might debate whether a supreme being is watching us, there is little doubt that cameras and other devices are. Video surveillance systems processing pictorial and audiovisual information are increasingly used. The public and private sectors use these technologies for various purposes, including enhancing security, providing audience analysis, delivering personalized services and displaying advertising. The intrusion into individuals' lives is becoming more and more pervasive.

The Guidelines are the Ark of Covenant from which organizations processing personal data through video devices could seek the "Ten Commandments" for obeying GDPR requirements. (Other prescripts might be imposed by domestic laws, though.)

If you are eager to learn these commandments, continue reading.

RETURN TO COMMANDMENTS LIST

1. Honor the GDPR, especially its basic principles

Organizations need to keep in mind the processing principles of Art. 5 GDPR—particularly those for purpose limitation and accountability. The purposes of processing should be documented in writing for every surveillance camera in use (although, if several cameras are used for the same purpose, they may be documented together). And the descriptions should be specific (e.g., "for your safety" might not be adequate to earn placement on the list for heaven).

Careful consideration should be also given to data minimization. The Guidelines make it clear that organizations should minimize the risk of capturing footage revealing sensitive data, regardless of the purpose.

RETURN TO COMMANDMENTS LIST

2. Remember to carry out a proper assessment if you rely on "legitimate interest"

A legal basis for the processing of personal data collected through video devices should always be identified. The Guidelines point out that Art. 6(1)(f) GDPR (legitimate interest) will often be the appropriate legal ground.

The EDPB gives steps on how to do this correctly: (1) identify the existence of legitimate interest, (2) establish whether the processing is necessary for the planned purpose and (3) perform the balancing test. No new mantra—save that for the EDPB the existence of a legitimate interest should be based on a real and present concern (not speculative or fictional); further, it should be backed by strong evidence. If a shop owner wants to install a video surveillance system to prevent vandalism, they have to show that there is a high risk of vandalism in the neighborhood (e.g., by presenting statistics concerning crimes in that area). In addition, organizations should reassess the existence of such a need on a regular basis.

The Guidelines require organizations to analyze whether the actual deployment is fit for the purpose and whether it will *actually deliver* on the expectations; fencing a property or providing better lighting may prevent property-related crimes without intruding on privacy.

When carrying out the balancing test (between the legitimate interests of the controller or those of a third party and the fundamental rights and freedoms of the data subjects), particular attention should be given to the "intensity" of the intrusion into individuals' rights and freedoms and to the individuals' expectations. The Guidelines state that the test is to be performed on a case-by-case basis (i.e., not by using a one-size-fits-all approach).

The EDPB is ecumenical on the use of other Art. 6 GDPR legal grounds, even if it is more agnostic to two of them: consent or necessity to perform a task carried out in the public interest. Further, consent must be *valid* consent; the Guidelines made it clear, for example, that entering a marked monitored area does not constitute a consent statement nor a clear affirmative action equivalent to consent.

.

RETURN TO COMMANDMENTS LIST

3. Thou shalt not disclose video footage to third parties without a separate legal basis

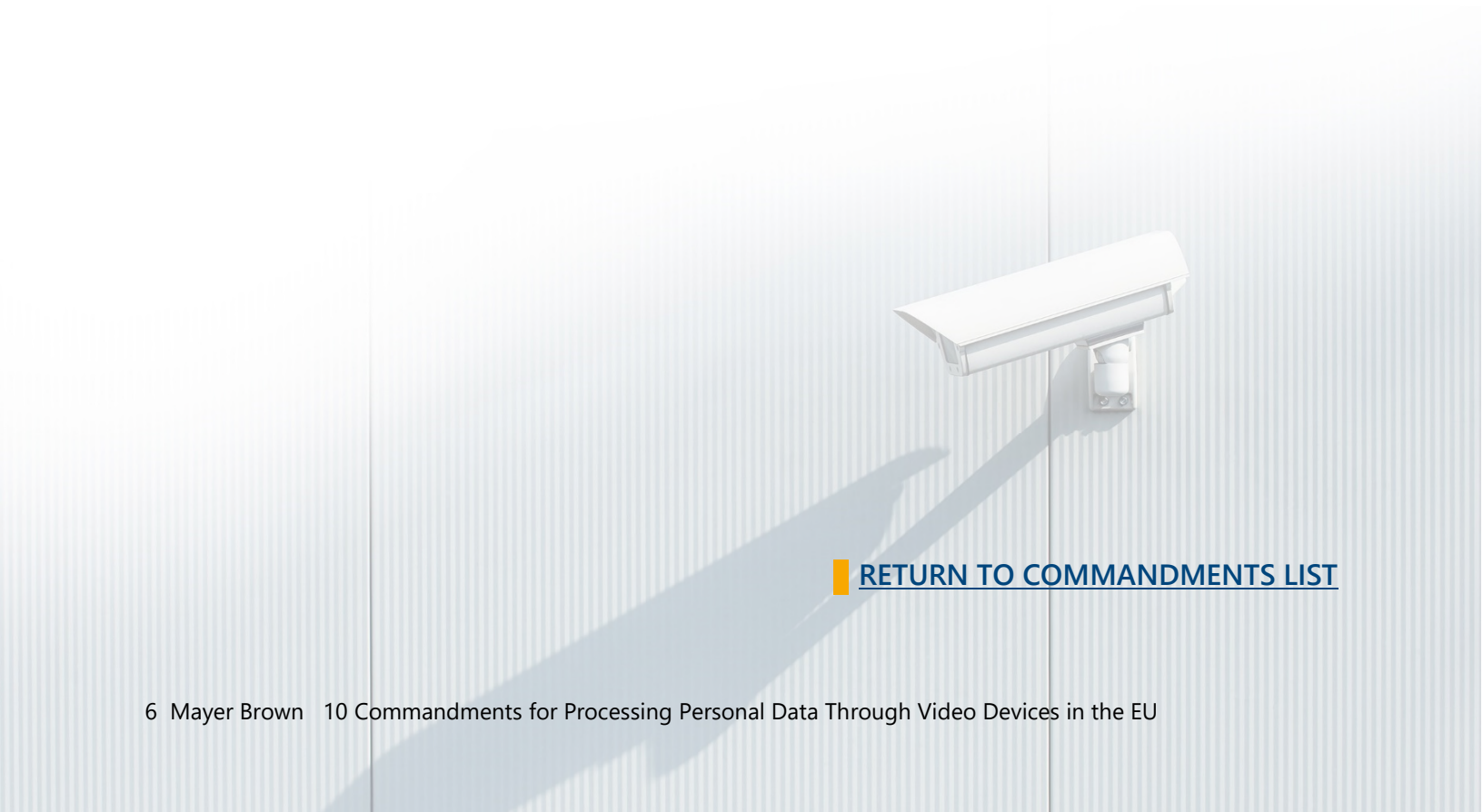
The EDPB underlines that any disclosure of video footage is a separate processing activity and hence requires the disclosing organization to identify a legal basis. This means that data controllers should identify a specific legal basis for sharing personal data, which may be different from the one used to collect and process—in particular when the purpose for disclosing the data does not appear compatible with the purpose for collecting it. For example, video footage collected for security purposes may be uploaded on the Internet only if the data controller obtained consent from data subjects.

RETURN TO COMMANDMENTS LIST

4. Remember that not every image is a special category

The Guidelines point out that not every video surveillance will be considered to be the processing of special categories of data.

The fact that footage shows a data subject in a wheelchair or entering a church is not enough to, by itself, qualify the footage as processing a special category of data; only when such a footage is processed to deduce special categories of data would Art. 9 GDPR apply.



RETURN TO COMMANDMENTS LIST

5. Thou shalt provide alternatives to biometric devices

The Guidelines point out that video footage of an individual is not in itself biometric data under Art. 9 GDPR if it has not been specifically technically processed in order to allow it to identify an individual. For instance, if a facial recognition system does not generate biometric templates in order to identify a person as a specific person—a unique individual—but rather detects physical characteristics in order to classify the person to a particular category of people, the processing does not fall under Art. 9 GDPR.

When an organization relies on biometric processing to provide access to its services, alternatives should be provided (without any additional costs or restraints for the users of the services). For instance, at the entrance of a building, badges or keys could be provided as alternatives to using a facial recognition/biometrics system. In addition, the Guidelines suggest that the facial recognition function should be triggered by the data subject proactively taking an action (e.g., by pushing a button).

RETURN TO COMMANDMENTS LIST

6. Honor the rights of data subjects

The Guidelines shed some light on the exercise of data subjects' rights in the context of the use of video surveillance.

With regard to the right to access, organizations might implement technical measures to minimize the possibility of violating the rights of others. Examples are image editing by masking or scrambling. In addition, the exercise of the right to access may be limited if the organization is unable to identify the data subject. For instance, if the video is not searchable for personal data, data subjects willing to exercise their right to access are to specify, apart from identification data, a reasonable timeframe when they entered the monitored area.

In relation to the right to erasure, the EDPB advises that the organizations might fulfill it by blurring the picture with no retroactive ability to recover the personal data that the picture previously contained.

With regard to the right to object, the EDPB clarifies that data subjects should be able to exercise it when entering, during the time in or after leaving the monitored area.

RETURN TO COMMANDMENTS LIST

7. Remember to comply with your transparency obligations

Transparency is ensured by using a layered approach composed of a first layer (a warning sign— which is often required by other laws, in any event) and a second layer (further details that are mandatory to display).

Warning signs should provide a meaningful overview of the intended processing of the footage. The warning should (i) be positioned in such a way that the data subject can easily see it before entering the monitored area (e.g., at eye level) and (ii) convey the most important information—e.g., purposes for processing the data and the controller's identity—as well as any other relevant information that the data subject would not otherwise know.

The second layer of information should be easily available, too—and without having to enter the monitored area. For example, this information could be published on a sheet available at an information desk in or on a poster hung at a reception area. Other ways to provide access to this information include phone numbers, QR codes and website addresses.

RETURN TO COMMANDMENTS LIST

8. Thou shalt not keep personal data indefinitely

Organizations cannot store the personal data obtained through video devices indefinitely. Unless there are some specific nationally prescribed storage periods (which, by the way, is often the case), the EDPB advises that the storage periods reflect the purposes for which the data was initially collected. For instance, the personal data collected for the purpose of detecting vandalism should be erased after a few days since this is usually the time that is needed to detect acts of vandalism. And the longer that an organization stores the data (especially if longer than 72 hours), the higher the burden of proof for the legitimacy and necessity of that storage.

RETURN TO COMMANDMENTS LIST

9. Remember to implement appropriate technical and organizational measures

The EDPB points out that appropriate organizational measures should be implemented prior to the collection and processing of video footage. The Guidelines emphasize that to protect privacy organizations should not use functions that are not necessary. For instance, unlimited movement of cameras, zooming, audio recording and radio transmission should be deactivated if they are not necessary.

With regard to the system and security measures, as well as access control, the Guidelines provide a useful, non-exhaustive list of measures that organizations might apply, including (i) data encryption, (ii) protection of the entire video surveillance system infrastructure against physical tampering and theft, (iii) detection of failures of components, software and interconnections and (iv) positioning video surveillance monitors in such a way that only authorized operators can view them.

RETURN TO COMMANDMENTS LIST

10. Remember to consider whether you need to carry out a DPIA

When implementing video surveillance systems, organizations should consider whether a data protection impact assessment ("DPIA") is required under Art. 35 GDPR and consult the list of processing operations that are subject to mandatory DPIA of their relevant supervisory authority. For the EDPB, and considering the traditional use of video surveillance, organizations should assume that many cases of video surveillance will require a DPIA.

RETURN TO COMMANDMENTS LIST

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

EU Contacts

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

UK Contacts

Mark A. Prinsley
+44 20 3130 3900
mprinsley@mayerbrown.com

Oliver Yaros
+44 20 3130 3698
oyaros@mayerbrown.com