# Guidelines on Video Surveillance and the GDPR Published by the European Data Protection Board

**TOPICS:** Video Surveillance, Biometric, Face Recognition, GDPR, EDPB, EU

The EDPB has published Guidelines on Video Surveillance ("**Guidelines**"), which clarifies how the GDPR applies to the processing of personal data when using video devices, including for biometric recognition.

The objective of the Guidelines is to ensure that guarantees are taken to avoid any misuse of video footage for different and unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.), or misuse of biometric and facial recognition technologies.

In this context, **the Guidelines clarify that the GDPR is applicable to video surveillance whenever an individual can be directly or indirectly identified.** This excludes the GDPR application where there is no reference to a person, such as when a video camera is integrated in a car for providing parking assistance, if the camera is adjusted in a way that does not collect any information relating to an identified person.

When using video surveillance technologies, a first factor of consideration must be the legal basis for processing data. **According to the Guidelines, the most likely legal basis is legitimate interest; however, the legitimate interest must be of real existence and has to relate to a present or imminent issue** (not fictional or speculative), such as showing reports or statistics of damages or serious incidents in the past.

In this context, **consent is not an appropriate legal basis for video surveillance in most cases**, as it is in the surveillance's nature that this technology monitors an unknown number of people at once. The Guidelines further indicate that in most cases consent is not a valid basis for surveillance of employees.

Before installing a video surveillance system, **it should be examined if this measure is suitable, adequate and necessary to attain the desired goal**. The controller is obliged to assess **where and when video surveillance measures are strictly necessary**, as other alternative measures could include fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better the controller, etc.

The controller must also ensure data minimization, which could be achieved by blocking out or pixelating irrelevant areas. Finally, a legitimate interest does not apply where the individual cannot reasonably expect to be subject to monitoring in a specific situation, e.g. in examination and treatment rooms, toilets, etc.

The Guidelines further note that **video surveillance may reveal data of a highly personal nature and sensitive data.** In this context, video surveillance cannot rely on the fact that the processing relates to personal data that is manifestly made public by the data subject, as the mere fact of entering into the range of the camera does not imply that the data subject intends to make public his or her sensitive data.

Another topic of focus in the Guidelines is the **use of video surveillance with biometric recognition functionality**, for purposes such as marketing, statistical or security, which in most cases require explicit consent of all data subjects. In that regard, **the facial recognition method should be triggered by the data subject himself, for instance by pushing a button.** In addition, **the controller must always offer an alternative way to access the service/building without biometric recognition.**

The Guidelines also highlight the transparency obligations, clarifying that the most important information, such as details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing, **should be prominently displayed on a warning sign at a reasonable distance from the places monitored, while further mandatory details may be provided by other means, such as a complete information sheet available at a central location.**

Finally, the Guidelines deal with the topic of data retention. In many cases (e.g. when used for detecting vandalism), the personal should be **erased, ideally automatically, after a few days.**

Several discussions and rulings regarding the use of recognition technologies have been trending. In our previous newsletter, we reported that San Francisco recently banned local government agencies' use of facial recognition, a move that is being followed by other US States.