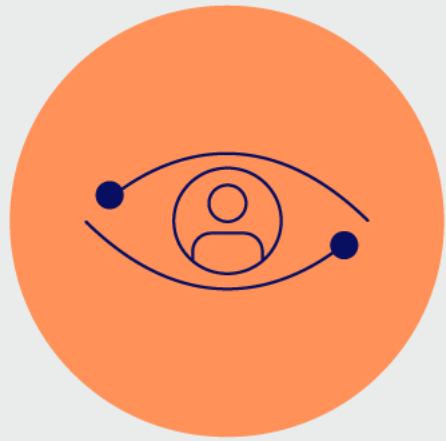


Video devices & data protection: When to act and what to do



April 2026

Compliance with the General Data Protection Regulation (GDPR) is mandatory for every organisation using video surveillance.

While individuals might be comfortable with video surveillance set up for certain security purposes, guarantees must be taken to avoid any misuse for totally different and unexpected purposes (e.g. marketing or employee monitoring).

The [EDPB Guidelines on processing of personal data through video devices](#) provide guidance covering lawfulness, disclosure of video footage to third parties, transparency, and the processing of sensitive data.



Lawfulness of processing

The legal grounds most likely to be used for processing video surveillance data are **legitimate interest** and **necessity to perform a task** carried out in the public interest or in the exercise of official authority. In rather exceptional cases, **consent** might also be used as a legal basis.

Legitimate interest

In order to invoke [legitimate interest](#), an organisation should reply positively to the three questions below:

1 Is there a legitimate interest by the organisation or a third party?

Not every interest qualifies as legitimate. As a general rule, the interest pursued by an organisation or a third party should be related to their actual activities and should not be contrary to EU or member state law. The legitimate interest should be clear and precisely articulated, and effective at the date of the data processing (not hypothetical).

2 Is the processing really necessary for the legitimate interest?

When deciding whether processing is necessary, the organisation must check if its goal can be achieved in a less intrusive way. Processing should only take place if it is strictly needed for that purpose, and only using the data relevant for that purpose.

3

Are the interests or fundamental rights and freedoms of individuals overridden by legitimate interest?

To rely on legitimate interest, the organisation must ensure that its interest is **not overridden by the individuals' interests or fundamental rights and freedoms**. This requires considering their reasonable expectations and putting in place measures to limit the impact of the processing.

Necessity to perform a task in the public interest or in the exercise of official authority

Video surveillance can be used when necessary to carry out public tasks or official duties. If the exercise of official authority does not allow it, processing may still be justified for reasons such as protecting the health and safety of visitors and employees. In all cases, the use of video respect individuals' rights.

Consent

For video surveillance, consent can only be used as a legal basis in exceptional cases because it typically involves monitoring many people at once, and that they all need to give valid consent.

Household exemption

The GDPR does not apply to processing by a natural person for purely personal or household activity. However, this is interpreted narrowly. If a home camera involving constant recording covers a public space (like the street) or a neighbour's property, the GDPR applies.

Principles in practice: Key steps for organisations

When implementing video surveillance, organisations must put data protection principles in practice, particularly **transparency**, **storage limitation**, and the protection of sensitive data.



1. Transparency (information obligations)

Individuals must be aware that video surveillance is in operation. The information should be provided in a layered approach:

- **First layer (warning sign):** A sign positioned at eye level before the individual enters the monitored area. It should contain the most important details: purpose of processing, identity of the data controller, rights of the individual, and where to find detailed information.
- **Second layer (detailed information):** A complete information sheet available at a central location outside the monitored area (e.g., reception) or digitally (via QR code or website link) containing all mandatory details under Art. 13 GDPR.

2. Storage limitation

Personal data should not be kept longer than necessary.

- **Retention period:** In general, damages can be detected within one or two days. Therefore, a storage period of a few days is often sufficient.

3. Processing sensitive data (biometrics)

Video surveillance involving biometric data (e.g., facial recognition) entails processing of so-called sensitive data. This requires a higher standard of justification, often explicit consent from the individual.

Practical examples

Here are specific scenarios illustrating how to apply these rules:

Example

(section 5.1, paragraph 85, page 20)

Context: A hotel uses video surveillance with facial recognition to automatically alert the hotel manager that a VIP guest has arrived. The VIPs have given prior consent to be in the database.



What to do: To use this system lawfully, you must obtain consent from all guests monitored, not just the VIPs. If you cannot get consent from everyone (e.g., other guests passing by), you must not use the system in a way that captures their biometric data.

Example

(section 3.1, paragraph 31, page 12)

Context: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities.



What to do: In this case, the rights of individuals clearly override the interest of the controller, therefore cameras cannot be installed there. In addition, video surveillance to prevent accidents in toilets is not proportional as individuals expect not to be monitored.

Example

(section 7.2, paragraph 119, page 27)

Context: A shop owner is monitoring his shop.



What to do: To inform individuals, the owner places a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easily accessible location in his shop.

Example

(section 6.1, paragraph 97, page 23)

Context: The organisation automatically deletes footage, for example after 2 days.



What to do: The organisation cannot supply footage to the individual after those 2 days. If the controller receives a request after those 2 days, the individual should be informed that the footage is no longer available.

Example

(section 3.1, paragraph 28, page 11)

Context: A bookshop wants to protect its premises against vandalism.



What to do: In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.



Your action plan for video surveillance compliance

Organisations are accountable for their surveillance systems. Use this checklist to demonstrate compliance:

Action point	Why it matters
Define the purpose and identify a legal basis	Clearly document why you need surveillance (e.g., “property protection” is too vague; specify “preventing theft in the warehouse”) and identify a suitable legal basis.
Inform	Inform individuals that they are being monitored by displaying clearly visible signage with a first layer of information, and by making more complete information easily accessible .
Define the storage period before erasing the data	Footage should be erased, ideally automatically, when it is no longer necessary for the purpose . For the purpose of detecting vandalism, a retention period of a few days should often be appropriate. In some member states, there may be specific provisions for storage periods with regards to video surveillance.
Secure the data	Ensure your system is secure . Implement technical measures (encryption, access control) and organisational measures (policies, training) to protect footage from unauthorised access.
Respect individual rights	Be ready to respond to requests for access or erasure . If a person asks for footage of themselves, you must provide it (potentially blurring others to protect third-party rights).
Conduct a DPIA if required	If the processing is likely to result in a high risk (e.g., systematic monitoring of a publicly accessible area on a large scale), you must conduct a Data Protection Impact Assessment (DPIA) .
Responsible disclosure	Disclose footage to third parties only if your legal basis allows it . Transmit it to law enforcement agencies only where this is justified .

By following the guidelines, you can use video devices effectively without infringing on fundamental rights.

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full guidelines.

[Read the complete guidelines](#)