Celab
COMMUNICATIONS

Body-worn cameras and legal considerations

What legal, organisational and practical considerations need to be addressed before the cameras are purchased and put into use?

Note

This article is not legal advice and does not replace an organisation's own legal assessment.

Body-worn cameras and legal considerations: questions to assess before implementation.

A growing range of organisations are considering the use of body-worn cameras, but implementation is not just a technical decision. What legal, organisational and practical considerations need to be addressed before the cameras are purchased and put into use?

Body-worn cameras are increasingly used in organisations where employees meet people in situations that may become pressured, confrontational or dangerous.

Outside law enforcement as well, more companies and organisations are considering the introduction of body-worn cameras. This may include public transport, rescue services, healthcare, retail and other working environments where threats, violence, vandalism, accidents or public order disturbances may occur.

Body-worn cameras may, for example:

- **help prevent escalation and contribute to greater safety**
- **improve documentation and strengthen evidence**
- **provide a basis for developing working methods after incidents**
- **increase transparency in exposed or difficult-to-assess situations**

At the same time, body-worn cameras involve the processing of personal data, often in situations where people have not chosen to be filmed. Introducing body-worn cameras is therefore not only a technical or operational issue. It also requires legal, organisational and ethical considerations.

The purpose of this article is to provide an overview of questions that organisations should, at a minimum, have assessed together with legal expertise, data protection officers, security managers or other relevant functions before body-worn cameras are purchased and put into use.

The article mainly focuses on organisations that are not law enforcement authorities, since law enforcement activities are subject to specific legal frameworks that are not covered here. Their conditions are defined, among other things, in the Swedish Criminal Data Act [Source 1] and in the EU Data Protection Directive for law enforcement, also known as the Law Enforcement Directive.

Note

This article is purely focused on aspects regarding implementation of body-worn cameras in Sweden.

Table of contents

Body-worn cameras are not the same as fixed surveillance cameras

At first glance, it is easy to assume that the use of body-worn cameras is regulated in the same way as fixed camera surveillance under the Swedish Camera Surveillance Act, SFS 2018:1200 [Source 2]. However, Section 3 states that the Act applies to cameras or comparable equipment that is not operated on site and that entails continuous or regularly repeated monitoring of people.

Because body-worn cameras are normally carried, activated and operated by a person on site, they normally fall outside the definition of camera surveillance in the Camera Surveillance Act.

That does not mean, however, that their use is unrestricted.

If the camera captures identifiable people, voices, vehicles or other information that can be linked to a natural person, the use may involve processing of personal data. The organisation must then comply with data protection rules such as the GDPR [Source 3] and other relevant national or EU legislation.

Are body-worn cameras allowed?

In other words, there is no general answer that applies to all organisations, roles and use cases. A more relevant question is therefore:

Under what conditions can our organisation use body-worn cameras for our purpose, in a way that is necessary, proportionate and documented?

Did you know?

The permit requirement for camera surveillance by businesses and organisations ceased to apply on 31 March 2025. Instead, an assessment must be carried out before surveillance begins, where the interest in carrying out the surveillance must outweigh the individual's interest in not being subject to it.

Even though body-worn cameras are normally not covered by the definition of camera surveillance under the Swedish Camera Surveillance Act, this change is still relevant as background. It reflects how camera surveillance in Sweden now relies to a greater extent on the organisation's own assessment and documentation. [Source 4]

Questions to consider before implementation

1. Define the purpose

The first step should be to define why the cameras are to be used, because an unclear purpose makes it difficult to assess the lawful basis and other essential conditions for the use.

Possible purposes may include:

- documenting threats, violence or public order disturbances
- strengthening the working environment for staff in exposed situations
- securing traceability and evidential value after incidents
- creating transparency during interventions, checks, inspections or other exposed encounters
- documenting the sequence of events in accidents, operational disruptions or security incidents
- improving the basis for investigation after an incident has occurred

However, the purpose must be precise.

Safety may be a legitimate objective, but to assess whether body-worn cameras are the right measure, the organisation must specify what the cameras are expected to contribute, in which situations they are to be used and what problem they are intended to solve.

Example: SL's use of body-worn cameras

The 2021 decision by the Swedish Authority for Privacy Protection (IMY) concerning Storstockholms Lokaltrafik's (SL) use of body-worn cameras shows why the purpose is decisive. In its assessment, IMY considered that activated recording of video and audio during ongoing threatening or violent situations could be necessary to achieve the purpose of preventing and documenting threats and violence. [Source 5]

This did not mean that SL's use as a whole was considered compliant with the GDPR. Several aspects of the use were criticised, which we return to later in the article.

At the same time, the authority did not consider the use of body-worn cameras to verify identity in connection with penalty fares to be necessary, and found that the privacy interest therefore carried greater weight.

The key lesson is that the same camera, with the same user and in the same environment, may be assessed differently depending on the purpose.

2. Clarify responsibilities and roles

Once the purpose has been established, the organisation must clarify who is responsible for the use of the body-worn cameras and for handling the recorded material and the data generated by their use.

Under the GDPR, responsibility is normally determined by who decides the purposes and means of the processing of personal data. Responsibility therefore normally lies with the organisation, or organisations, that decide why the cameras are to be used and how the use is to take place. In other words, the person carrying the equipment is not necessarily responsible for the processing of personal data.

In some cases, the allocation of responsibility is straightforward. In others, several actors may be involved, such as an employer, a client, a security company, a municipal organisation, a property owner, a system supplier or a cloud service provider.

It must then be clear who is the data controller, whether any party acts as a processor, whether several actors have joint responsibility, and which agreements, instructions or internal procedures are required.

Questions to assess include, for example:

- **Who decides the purpose of the cameras?**
- **Who is responsible for ensuring that the use is necessary and proportionate in relation to the purpose?**
- **Who decides when and how the cameras may be used?**
- **Who is responsible for providing information to people who may be filmed?**
- **Who is responsible for storage, access, disclosure and deletion?**
- **Who may access recorded material?**
- **Are there external suppliers that process material on behalf of the organisation?**
- **Are there specific regulations, agreements or internal instructions that affect the allocation of responsibility?**

The concrete and practical issues relating to recording, information, storage and similar matters are addressed in the following sections. The important point at this stage is to ensure that responsibility does not fall between functions, suppliers or organisational levels.

Unclear responsibility risks becoming no practical responsibility at all.


MOTOROLA
HSC

3. When and how is the camera used?

One of the most central questions is when and how the cameras are to record. Body-worn cameras can be used in several ways: continuous recording, manual activation, automatic activation, pre-recording or recording only in defined situations.

Continuous or recurring recording increases the risk of capturing people who have no connection to the situation the camera is intended to document, such as passers-by, employees, customers, patients, service users or children who happen to be present.

As a result, the broader and longer the recording, the greater the risk of privacy intrusion. It is also likely to become more difficult to demonstrate that the recording is necessary and proportionate in relation to the purpose.

The organisation therefore needs to consider, for example:

- whether the camera should be active at all times or only start when needed
- who is allowed to start recording
- in which situations recording may or must take place
- whether recording should be voluntary, recommended or mandatory for the user
- whether the camera should have pre-recording
- whether recording should be started automatically by an external system, an alarm, a person or another predefined event
- how and when recording should be ended
- how accidental or incorrectly started recordings should be handled

A practical starting point is that recording should be linked to clearly defined situations, such as threats, violence, public order disturbances, accidents or other events where documentation is necessary to achieve the defined purpose.

Pre-recording requires particular consideration. The function means that the camera continuously buffers a short sequence that is then saved when recording is activated, which means the material can also show what happened before the active recording. The purpose is to capture the sequence of events even if the user does not have time to press the record button immediately. The function can be operationally valuable, but it also means that the camera processes data before active recording begins.

The organisation should therefore be able to justify at least the following:

- **why pre-recording is needed**
- **how long the pre-recording should be**
- **whether it should include video, audio or both**

Example: SL's use of pre-recording

In the Swedish Authority for Privacy Protection's (IMY) decision following its supervision of SL, the authority considered that one minute of pre-recording was too extensive in the use case in question. IMY found that a shorter period, of no more than 15 seconds, could have been accepted in that specific case. [Source 5]

This does not mean that 15 seconds is a general upper limit for all organisations. However, the decision shows that pre-recording should be assessed separately and that the organisation must be able to justify the function, its scope and its duration.

4. Audio recording should be assessed separately from video recording

Body-worn cameras can often record both video and audio, but this does not mean that both functions should automatically be used in every situation.

In the previous section, we highlighted that broad and lengthy video recording can increase the risk of capturing people who are not relevant to the situation the camera is intended to document. In the same way, audio recording may capture conversations, comments and sensitive information from or about patients, service users, customers, employees or other people who may not even appear in the image.

Audio recording can therefore involve a greater privacy intrusion than video recording alone. At the same time, threats are often verbal, which may mean that audio recording can, in certain situations, be considered necessary and proportionate. The organisation should therefore assess audio separately from video.

Questions to assess include, for example:

- **Is audio needed for the specific purpose?**
- **In which situations is audio necessary?**
- **Should audio be enabled by default, or only enabled after a specific decision?**
- **Can video be used without audio in some situations?**
- **How are conversations with people who are not directly involved in the incident handled?**
- **Is there a risk that sensitive personal data will be captured through audio recording?**
- **Should the user be able to disable audio?**
- **Should audio always be included when material is exported or shared, or should it be possible to limit it?**

It is therefore important to distinguish between what the technology can do and what the organisation should do. The fact that a camera supports audio recording does not mean that audio is always necessary or proportionate.

The same reasoning should also apply to other technical functions, such as:

- **automatic activation**
- **location data and positioning**
- **livestreaming and remote access**
- **metadata**

Each function should be assessed in relation to purpose, benefit, risk and proportionality.

Example: SL's use of audio recording

In its decision following supervision of SL, the Swedish Authority for Privacy Protection (IMY) considered that activated recording of audio and video during an ongoing threatening or violent situation could be necessary to achieve SL's purpose of preventing and documenting threats and violence [Source 5].

At the same time, the decision shows that audio recording should be assessed separately in relation to each purpose and use situation.

5. Information must be provided when recording takes place

As with other collection of personal data, information must be provided when personal data is collected through body-worn cameras under Article 13 of the General Data Protection Regulation (GDPR). The people who may be included in the recording must therefore receive clear information about the processing of their personal data. [Source 3]

For fixed cameras, information is usually provided through signage. Because body-worn cameras move with the user and are often only activated during specific events, the information situation becomes more complex.

The organisation therefore needs to assess how information should be managed and provided in practice.

This may include, for example:

- a clearly visible camera
- a clear recording indicator
- marking on a uniform, vest or equipment
- verbal information when possible and appropriate
- signage in premises, vehicles or entrances
- information cards
- a QR code linking to more detailed information
- a web page with information about the processing of personal data
- a contact route to the controller or data protection officer
- internal procedures for when and how information is to be provided

It is not necessarily enough that the camera is visible. The data subject must be able to understand who is responsible for the processing, why recording takes place, what data is processed, how the material is handled, how long it is stored and what rights the data subject has.

At the same time, the information model must be realistic. In a threatening, urgent or safety-critical situation, it may be inappropriate or impossible to provide complete verbal information before recording starts. The organisation should therefore use several layers of information, such as a combination of advance information, clear indicators and supplementary information channels.

The image is only a visualisation and not an example of approved signage.

Example: SL's information during recording

Following its supervision, the Swedish Authority for Privacy Protection (IMY) considered that SL had failed to provide adequate information about both video and audio recording. People who were issued a penalty fare received detailed information about the processing of personal data, with current links to further information on the receipt, which IMY described as part of the supplementary information (layer 2). This meant that other passengers who were recorded did not receive equivalent information. In other words, passengers could have been captured by the camera without being the actual subject of the ticket inspection or incident, while having a valid ticket and posing no threat.

IMY also found that the signage and markings intended to constitute "layer 1" were insufficient. [Source 5]

Later review

Following an appeal to the Administrative Court of Appeal, the administrative fine was set aside in the part concerning the information obligation, because the court held that Article 13 was not applicable in the situation in question. IMY then appealed to the Supreme Administrative Court, which requested a preliminary ruling from the Court of Justice of the European Union. The Court of Justice later confirmed IMY's interpretation that Article 13, not Article 14, applies when personal data is collected through body-worn cameras.

[Source 6], [Source 7]

6. Storage and handling of material

Introducing body-worn cameras is not only about when recording may take place. Just as important is what happens to the material afterwards.

Recorded material may contain video, audio, metadata and logs. It may also show people in vulnerable, confrontational or sensitive situations. Before implementation, the organisation therefore needs to decide how the material will be transferred, stored, used, protected and ultimately deleted or disposed of.

A fundamental starting point is that material should not be stored for longer than is needed for the defined purpose. [Source 8]

A recording that shows an actual incident may need to be handled differently from a recording that was started by mistake or that does not show any relevant event.

The organisation therefore needs to consider, for example:

- where the material will be stored
- whether storage will be local, cloud-based or hybrid
- how the material is transferred from the camera to the storage system
- how the material is protected during transfer
- whether external suppliers process material on behalf of the organisation
- whether data processing agreements are required
- how long different types of material are to be stored
- when material is to be deleted, disposed of or, where relevant, archived
- who may view recorded material
- who may edit, mask or otherwise process material
- who may export, share or disclose material, and through which approved channels
- how export or disclosure from the storage system is to take place securely
- whether and how access and actions are to be logged
- how the material is protected against unauthorised access
- how material that may be needed as evidence is to be handled
- how accidental or incorrect recording is to be handled
- how the organisation handles requests from data subjects

Access and use should be limited to the people and functions that need the material for a clearly defined purpose. It should therefore not be possible for all managers, administrators or users to view, process or export material simply because they have a role in the organisation or technical access to the system.

It is also important to distinguish between storing material and using material. A recording may need to be stored for a limited period, but that does not mean it can be freely used for purposes other than those on which the recording was based.

If material is to be shared, exported or passed on, the organisation needs procedures for who may decide this, through which channels it may take place, and whether parts of the video or audio need to be masked. Informal working methods, local copies, email attachments or uncontrolled file transfer can create risks that should be managed through both procedures and technical configuration.

For public-sector organisations, additional rules may affect the handling of the material, such as rules on public records, secrecy, archiving, disclosure and retention or disposal.

By deciding on transfer, storage and handling before implementation, the organisation reduces the risk that material is stored for too long, used for the wrong purpose, shared in the wrong way or made available to more people than necessary.

7. Also address the employer perspective

So far, the article has mainly addressed how body-worn cameras can affect people who are filmed, but they are not the only people affected. The person carrying the camera is affected as well.

For some employees, the camera may be perceived as support and contribute to a safer working situation. For others, it may be perceived as a control tool, especially if there are uncertainties about use and follow-up.

The employer perspective therefore also needs to be addressed before implementation [Source 9].

The organisation should clarify, among other things:

- which roles or functions will carry cameras
- whether use is voluntary, mandatory or situation-based
- when the camera must or may be activated
- when the camera must not be used
- whether the employee may start and stop recording themselves
- whether recorded material may be used for training and follow-up
- whether material may be used in management or internal investigations
- who may review material in which employees appear, and for what purpose
- how users are trained in procedures, limitations and responsibilities
- how safety representatives, trade union representatives, HR or work environment functions should be involved
- how the organisation avoids the cameras being perceived as general staff surveillance

It may be reasonable to use recorded material to understand and follow up actual incidents, if this falls within the defined purpose and the procedures decided by the organisation. The material can provide a better basis for training, procedures and preventive work. But this should be distinguished from ongoing monitoring of employees' everyday work.

A practical starting point is to define the difference between incident-related follow-up and general performance monitoring. Using material to follow up incidents and improve procedures may be justified, but using it to continuously review how staff perform their work requires a separate and significantly more restrictive assessment.

Clear internal rules, internal anchoring and training are therefore important. Employees need to know when the camera is to be used, when it is not to be used, what happens to the material afterwards and in which situations the material may be reviewed.

A well-executed implementation is therefore not only about informing the people who may be filmed. It is also about building trust among the employees who will carry the equipment and use it in practice.

8. Technology should support legal compliance

The right technology does not replace the legal assessment. However, the right technology can simplify implementation and, in some cases, create basic conditions for an implementation that is appropriate, proportionate and secure.

Although image quality, frame rate and colour reproduction are important technical characteristics, implementing body-worn cameras is not only about these factors. Body-worn cameras are part of an ecosystem of equipment, applications and system architecture that must work together and be assessed as a whole, based on their ability to support the organisation's legal, organisational and operational conditions and requirements.

Relevant functions may include, for example:

Recording, configuration and user support

- resolution, optics, recording frame rate and field of view
- battery life, robustness and ease of use
- choice of continuous, automatic, remote, event-triggered or manual recording
- indication when recording is in progress
- ability to control audio recording separately
- active, limited or disabled pre-recording
- encryption, watermarking and tamper protection to support the chain of custody
- support for configuration and management of metadata and traceability

Collection, transfer and storage

- secure transfer from camera to storage system
- encryption of material
- automatic deletion from the device after upload
- choice between local storage, cloud storage or a hybrid solution

Access, logging and editing

- role-based access
- logging of access and actions (traceability)
- editing or export requiring multi-level approval, for example according to the four-eyes principle or hierarchical approval

Retention, sharing and export

- support for retention and deletion rules
- ability to mask irrelevant video and audio information before sharing
- secure and encrypted export of material

Administration, management and configuration parameters

- remote configuration and management
- management of tens, hundreds or thousands of cameras from the same interface

A fit-for-purpose system for body-worn cameras should be able to support the considerations the organisation has already made. In this sense, body-worn cameras should not be viewed merely as stand-alone equipment worn on the body. They are part of a system for collecting, handling, protecting and using potentially sensitive material.

9. Document assessments, technology choices and procedures

Once the organisation has considered the different perspectives, the assessments and decisions need to be documented, unless this has already been done continuously.

Documentation is important for several reasons. It makes it easier to follow up use, train employees and demonstrate that the implementation is not based on a general desire for more recording, but on clearly defined needs and trade-offs.

The organisation should document, among other things:

- what purpose the cameras will have
- which lawful basis is relied upon
- who is the data controller
- whether processors or external suppliers process material
- when the cameras may and may not be used
- whether audio recording is used and in which situations
- whether pre-recording is used and how it is configured
- how information is provided to people who may be filmed
- how material is transferred, stored, protected, used and deleted
- who has access to material and for which purposes
- how export, sharing, masking and disclosure may take place
- how employees are informed, trained and involved
- how the chosen technology supports the agreed procedures and limitations

The technology choice should therefore also be included in the documentation. If the organisation chooses a system with, for example, audio recording, pre-recording or export functions, the documentation should show why these functions are needed, how they are linked to the purpose and what limitations have been introduced to reduce the risk of privacy intrusion.

An important part of implementation is therefore to move from assessment to working practice. It is not enough that the technology can be used correctly. The organisation must also ensure that users know when, how and why the cameras are to be used, and that responsible functions can follow up compliance with the procedures.

The documentation must therefore also be translated into practical procedures, such as training, instructions, matrices, checklists and report templates.

The documentation should also be kept up to date. If the purpose or other operational, technical or legal conditions change, previous assessments may need to be reconsidered and the documentation updated accordingly.

In this way, the documentation becomes more than a legal record. It also becomes a practical tool for ensuring that body-worn cameras are used in a controlled, fit-for-purpose and well-anchored way.

Is a data protection impact assessment needed?

In some cases, the organisation may need to carry out a data protection impact assessment before body-worn cameras are introduced. Under the GDPR, a data protection impact assessment is required when a type of personal data processing is likely to result in a high risk to the rights and freedoms of natural persons.

The purpose is to identify risks in advance and assess which measures are needed to protect the people who may be affected by the processing.

A data protection impact assessment should not be seen as a mere formality. It can serve as a practical tool for assessing whether the implementation is reasonable, whether the use is sufficiently limited and whether the technical and organisational safeguards are adequate. [Source 10]


MOTOROLA
WARNING
3:18 / 08:54
MOTOROLA


06/05/2024 14:40:28
GRAPH VIEW
SYNC
MOTOROLA

Summary

Body-worn cameras can be a valuable tool and relevant support for organisations where employees meet people in pressured, confrontational or dangerous situations. They can contribute to greater safety, transparency and better follow-up after incidents.

However, implementation is not only about choosing cameras and systems. It is about defining the legal, organisational and practical conditions required to record and handle the material in a necessary, proportionate and secure way.

The central question is therefore not only whether body-worn cameras may be used, but under what circumstances the specific organisation can use them.

The clearer these considerations are before implementation, the better the conditions for using the technology in a way that creates value without making the privacy risks greater than necessary.

Checklist before implementation

As support for this work, we have compiled a checklist of questions that the organisation should go through before implementing body-worn cameras. The checklist can be used as a basis for internal dialogue, requirements specification, documentation and further legal assessment.

Download the checklist as a PDF (Swedish).

Sources

#	Source / Link *(Swedish)*
1	Brottsdatalag 2018:1177 (EU Law Enforcement Directive)
2	Kamerabevakningslagen, SFS 2018:1200
3	Europaparlamentets dataskyddsförordning, 2016/679 (GDPR)
4	Integritetsskyddsmyndighetens (IMY) information om regler för kamerabevakning
5	Integritetsskyddsmyndighetens (IMY) beslut efter tillsyn hos SL
6	Kammarrätten dömer i mål mellan SL och Integritetsskyddsmyndigheten
7	Klargörande från EU-domstolen rörande information vid kamerabevakning
8	Integritetsskyddsmyndigheten (IMY) grundläggande principer för personuppgifts-behandling
9	Integritetsskyddsmyndigheten (IMY) kontroll och övervakning av anställda
10	Integritetsskyddsmyndigheten (IMY) Konsekvensbedömning enligt GDPR

About Celab

+46 (0)303 24 60 00
info@celab.se
https://celab.se

Celab Communications AB is a Swedish company within the Tången Group that, since its founding in 1978, has achieved significant success in mission- and business critical communications.

By this, we mean solutions for organizations where reliable communication is essential to operational success and/or employee safety.

The company's foundational idea is to provide communication systems based on world-leading equipment, which, through our unique expertise, are developed, refined, and optimized specifically for our customers and their unique operations.

Celab COMMUNICATIONS

HQ Rollsbovägen 20, 442 40 Kungälv
Stockholm Elsa Brändströms gata 56, 129 52 Hägersten
Karlstad Lagergrens gata 2, 652 26 Karlstad