LOGENT
SUPPORTING LOGISTICS

2024

CCTV Policy

Group-wide, summary policy (GDPR and the Camera Surveillance Act)

Administered by: HR Department
Approved by: CEO Logent Group
Valid from: 2024-02-06
Valid until: Until further notice

LOGENT
SUPPORTING LOGISTICS

1. Purpose

The purpose of this policy is to set out Logent's common framework for CCTV (camera surveillance) in the business. CCTV may only be used where there is a clear need (e.g. security/safety) and where the intrusion into privacy is proportionate. The policy is intended to ensure compliance with the GDPR and the Swedish Camera Surveillance Act and to create consistent handling across sites.

2. Scope

This policy applies to CCTV that Logent operates or is responsible for in premises, on fenced areas and other locations used in Logent's business. The policy applies to employees, temporary staff/consultants, visitors and others who may be captured by CCTV.

3. Definitions

- CCTV (camera surveillance): surveillance carried out with camera equipment, with or without recording.
- Footage/material: image material (and where applicable audio) captured through CCTV.
- Balancing test: a documented assessment of whether the surveillance interest outweighs the individual's interest in not being monitored.
- Record: a register containing certain information about CCTV that is carried out or has ceased (see Appendix B).

4. Key principles

- CCTV is never used to routinely monitor employees' work performance.
- CCTV must be necessary for a legitimate purpose and carried out to the minimum extent required.
- Less intrusive measures should be considered first (e.g. locks, alarms, lighting, procedures).
- CCTV must not be used in areas where the privacy intrusion is normally particularly significant (e.g. changing rooms, toilets and break/lunch rooms).
- As a main rule, audio recording is not used.
- Any access is strictly limited (need-to-know) and all handling must be traceable.

Audio recording exception:

- Any deviation requires a specific assessment and a written decision by Legal and IT/Information Security, an updated balancing test and, where required, a DPIA.

5. Permitted purposes

CCTV may only be used for clearly defined purposes, for example to:

- Prevent and investigate crime, theft, unlawful intrusion and sabotage.
- Prevent, detect and investigate accidents and serious work environment incidents.
- Protect employees and visitors in threatening situations or violence.

- Protect particularly theft-attractive property or critical areas/processes.

Purpose and scope must be documented in the balancing test (Appendix A).

6. Lawful basis

For Logent's operations, the typical lawful basis for CCTV is legitimate interests (GDPR Article 6(1)(f)). CCTV cannot normally be based on consent in an employment relationship.

7. Balancing test and DPIA

Before CCTV is started or materially changed, Logent must carry out and document a balancing test (Appendix A). The balancing test must be updated if the risk profile changes, if the purpose changes or if the scope changes.

Where CCTV is likely to result in a high risk to individuals' rights and freedoms, Logent must carry out a Data Protection Impact Assessment (DPIA) under the GDPR before the processing starts. Where necessary, Legal/Data Protection must be involved.

8. Record of CCTV

For operations that are subject to a legal requirement to keep a record, Logent must keep a record with certain information about CCTV that is carried out, or that has ceased within the last five years. Logent may also keep such a record for all sites as part of group governance and GDPR compliance.

The record must be kept up to date. Information about ceased CCTV is retained in the record for up to five years (and to the extent required under applicable rules) so that Logent can demonstrate compliance and manage follow-up and supervision.

9. Information and signage

Logent must provide clear information about CCTV through signage at each entrance to the monitored area and before anyone enters the area. The sign must contain the most important information, and Logent must also provide more complete information (e.g. via intranet/website or a QR code on the sign). See Appendix C.

For new hires and when changes affect the workplace, information about CCTV must be included in the relevant onboarding/communication flow.

10. Access, handling and security

Access to CCTV footage must be limited to authorised roles, typically:

- Appointed security/facility responsible person or equivalent function.
- IT/provider for operation and troubleshooting (as processor) under agreement and instructions.
- HR/Legal to the extent required for investigations of incidents/cases.

All access must be traceable (logging) and footage may only be reviewed when needed for an approved purpose. Copying/extraction must be documented and stored securely with restricted access.

Periodic review (access rights and logs)

- Access rights to CCTV environments and recorded footage must be reviewed at least annually (recommendation: semi-annually) and documented.
- Access logs must be reviewed regularly (at least quarterly or as needed) and documented (date, scope, deviations, actions).
- For copying/extraction/disclosure, traceability must be ensured through documentation: who, when, why, which footage, recipient and case ID.

Suppliers, cloud services and remote access

- The storage location (country/region) must be known, documented and approved by IT/Information Security before go-live.
- Any remote access must be documented (who, why, how), restricted and protected (e.g. MFA and least privilege).
- A data processing agreement must be in place with the supplier. For transfers outside the EU/EEA, SCC and, where required, a TIA/supplementary measures must be applied.
- Security requirements must meet Logent's IT security requirements, including encryption in transit and at rest, logging and incident reporting.

11. Retention and deletion

Recorded footage must be retained for as short a time as possible and only as long as needed for the purposes. As a starting point, rolling retention is used, depending on the risk profile and need. Footage needed for an incident investigation may be kept longer, but only for as long as the case requires and with documented grounds.

Retention time per site must be stated in the balancing test and in signage/complete information.

12. Disclosures

CCTV footage may be disclosed to law enforcement authorities or other recipients where there is a lawful basis, for example in case of suspected crime or a serious incident. Disclosures must be documented (who, when, what, why).

13. Data subject rights

Individuals captured by CCTV have rights under the GDPR (e.g. the right to information and access). Requests are handled via Logent's data protection contact: it@logent.se. Logent may need to verify identity and performs confidentiality and privacy assessments, especially where footage includes multiple individuals.

Procedure for access requests to CCTV footage (summary)

- Requests are received via the data protection contact and recorded with a case ID. Identity is verified.
- Requests are narrowed (e.g. time and location) to minimise privacy intrusion and to make searches efficient.

- Where footage includes other individuals, their privacy is protected through masking/redaction or limiting disclosure.
- Requests may be wholly or partly refused if disclosure would adversely affect others' rights/freedoms or where another valid restriction applies.
- Complex cases are escalated to the Legal/DPO function in accordance with internal procedures.

14. Roles and responsibilities

- Controller: the relevant Logent company that conducts CCTV at the site (unless otherwise stated).
- Document owner: IT/Information Security (coordination) in cooperation with HR and Security/Facility.
- Site management: responsible for local compliance, that signage is in place and that local documentation (balancing test, record) is kept up to date.
- Suppliers: act as processors where they process footage on Logent's behalf and must be covered by a data processing agreement.

Decision-making and governance

- Decision on new/changed CCTV: the Site Manager proposes; decision is made by Legal after an approved balancing test.
- Owner of the record and balancing tests: IT or Legal is the record owner and ensures templates, storage and version control.
- Approval of access to recorded footage: Legal (primary), requiring a documented case ID and purpose. HR may be co-approver in employee relations matters/disputes.
- Periodic follow-up: IT ensures that annual (or semi-annual) controls are carried out and documented (see Periodic review).

15. Follow-up and revision

This policy must be reviewed at least annually or when regulations change, when the risk profile changes or when significant changes to CCTV are made. Each site is responsible for updating the balancing test and record when changes occur.

Appendix A – Template: Documented balancing test (CCTV)

Fill in per site/area/CCTV solution. Store in the central document management system.

1. Description of the surveillance

- Location/area monitored (address/site name):
- Type of location (e.g. warehouse, entrance, loading bay, parking):
- Purpose(s) of the surveillance (from section "Permitted purposes"):
- Scope: number of cameras, live monitoring yes/no, audio yes/no:
- Capture area: (describe and attach map/floor plan if needed):
- Retention time (rolling):

2. Surveillance interest (need)

- Which risk/incident is addressed? (e.g. theft, intrusion, work environment incidents):
- Incident history/statistics supporting the need:
- Consequences if CCTV is not used:

3. Alternative, less intrusive measures

- Which alternatives have been tested/considered? (alarms, locks, lighting, procedures, guards):
- Why are the alternatives not sufficient?

4. Privacy impact and safeguards

- Which individuals may be captured? (employees/visitors/vehicles):
- Are there sensitive areas nearby? (changing rooms/break areas):
- Masking/cropping of image?
- Access roles, logging and handling of extracts/copies:
- Information measures (signage + complete information):

5. Conclusion and decision

- Overall assessment: does the surveillance interest outweigh the privacy intrusion?
- Decision-maker and date:
- Plan for follow-up/review (at least annually):

Appendix B – Template: Record of CCTV

Add one row per monitored location/CCTV solution. Store and update on an ongoing basis.

Site/location	Address/site name	Type of location	Purpose	Number of cameras	Retention time	Start date	End date (if ceased)

Appendix C – Sign content and complete information

The sign (short information) should as a minimum state:

- That the area is under CCTV surveillance.

- Who is conducting the surveillance (Logent + relevant company).
- Contact details (GDPR email/phone).
- The purpose of the surveillance.
- Retention time (rolling) and whether footage is stored outside the EU/EEA (if applicable).
- Where complete information can be found (QR code/link).

Complete information (e.g. on intranet/website) should include:

- Controller and contact/DPO.
- Lawful basis (typically legitimate interests) and a short description of the balancing test.
- Purposes, monitored areas and any live monitoring.
- Recipients/processors (e.g. security supplier) and any transfers outside the EU/EEA.
- Retention and deletion.
- Data subject rights and how to submit a request.