

PRO-0033.01 Video-surveillance at the ECHA premises

1. Purpose

Video-surveillance is used to maintain the security and safety of ECHA, its staff, visitors and other persons as well as to protect the building, assets and information of the Agency.

This procedure defines the practical implementation of video-surveillance at the Agency while at the same time protecting the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

2. Scope

The procedure covers video material produced by surveillance systems in the ECHA premises.

The recording and broadcasting of events, meetings and trainings as well as video conferencing and video-entry systems (door-phones) are excluded from the scope.

1. Work Programme Activity: 14 Human resources and corporate services

2. Process Area: 14.11 Physical security

3. Sub-process: 14.11.2 Security technology

3. Description

Video-monitoring is an important tool in protecting the staff, visitors and assets of ECHA. It is used to deter security incidents from happening, detect them when they happen and to manage and investigate security incidents. Video-surveillance will not be used for performance assessment and appraisal of the staff. The data shall only be used in disciplinary proceedings in exceptional cases, when the images captured demonstrate a physical security incident or criminal behaviour.

Cameras are installed to control entry into the building and to monitor the outer shell of the ECHA premises. Within the building entry and exit-points are monitored as well as certain secure areas.

Cameras will not monitor areas where high privacy is expected and monitoring of areas outside the ECHA premises is limited to a minimum so that the objectives of the ECHA's security policies can be achieved.

The video-surveillance will also be used to monitor evacuation of the building and to complement the access control system, especially outside the office hours.

3.1 Coverage

The area where video-surveillance benefits security most include

- Entry and exit points into the ECHA premises;
- Areas where ECHA is responsible for the safety and security of its guests;
- Areas where the use of other security measures needs to be supplemented with video-surveillance.

These areas will be provided with most cameras and cameras with a very high technical quality.

Areas where video-surveillance is clearly beneficial to security include:

- Entry and exit points to the office areas or other non-public areas within ECHA premises;
- Outer shell of the buildings and their immediate vicinity;
- Secure areas within the premises;
- Points with an increased likelihood of break-in, vandalism or other specified threats to ECHA security;
- Evacuation exit routes (primary and secondary).

These areas will have video-surveillance unless the compensating security measures are considered adequate and the Security Manager so decides.

Video-surveillance will not be used in the following areas and their immediate entry points even if an area is indicated above.

- Areas where staff can expect high level of privacy such as leisure areas (canteen, kitchenettes, lounge areas, waiting rooms etc.), toilet facilities, dressing rooms, the gym area, the staff club room, as well as the office of the medical advisor and the office of the staff committee;
- Individual offices and open space office areas.

Cameras in the vicinity of increased privacy areas are focused and positioned so that these areas are not monitored.

3.2 Technology used

Video-monitoring is performed 24 hours a day, every day of the year. The total number of cameras in place at the date of adoption of this procedure is 69.

All monitoring cameras will be recording ones, but no sound recording is taking place. The video-surveillance system will not be interconnected to any other system.

No covert video-surveillance, nor infrared cameras, nor ad hoc monitoring will be used.

All cameras will have a resolution and image quality that enables identifying individuals, but no facial or behavioural recognition methods will be used.

Panning, zooming and/or tilting cameras will be used in areas where the area monitored is so wide and/or deep that otherwise the number of cameras needed would be excessive.

Cameras will be positioned so that they cannot be easily damaged or their view obstructed. Cameras mounted outdoors will be protected from the elements and provide a good picture

even in adverse weather conditions.

3.3 Responsibilities and access rights

The Security Manager is responsible for the implementation of this procedure. He/she will approve any exceptions, and consult the Data Protection Officer (DPO) where appropriate.

The number of users of the system is kept to a minimum, and includes:

- The in-house security staff

The Corporate Services Unit is responsible for the system and its Head of Unit nominates the system owner, main administrator and the access control manager (can be the same person).

- The Access Control Manager is responsible for the access right management;
- The main administrator has full access to the system;
- The system owner is responsible for system management issues.

The Physical Security Assistant can read, copy, move and delete video material as instructed by the Security Manager. With the main administrator he is responsible for the safe retention and deletion of the files, and together with the access control manager on the access privileges.

- The external security guards can watch live video; they can pan, tilt and zoom cameras if there is a security related reason to do so. They do not have direct access to video footage (files recorded by the camera).

The security guards' supervisor will monitor the use of the video-surveillance system and instruct on its proper use. He/she will inform the Physical Security Assistant of

- Suspected abuse of the video-surveillance system;
- Cameras which are not working, poorly placed or focused or otherwise do not increase security or put data protection at risk;
- Suspected security incidents where video material should be kept after the normal retention period;
- Requests of public authorities to access or transfer video material.

In a case of an immediate investigation of a suspected security incident, he/she can be granted with a temporary access to the stored video footage.

An up-to-date list of all persons having access to the system (including their level of access rights) is stored by the Physical Security Assistant at all times.

3.4 Storage

The video-surveillance system is a standalone and recordings will thus be stored on a system not connected to ECHA's local network.

Back-up copies of the system files are taken, but not of the video footage files.

System logging is set to monitor the usage to detect misuse and the users are informed about this.

The servers storing the recorded images are located within secure premises and protected by physical security measures.

3.5 Retention period

The normal retention period is 28 calendar days (4 weeks). The period has been defined based on the experiences gathered operating the system. Footage of peaceful demonstrations in the vicinity of the building shall be deleted within 2 hours of the end of the protest at the latest.

If a security incident is investigated, the Security Manager can decide on a longer retention period on case-by-case basis.

A register is kept by the Physical Security Assistant of all video-recording material retained after the normal retention period.

After 28 days the camera recording files are automatically and permanently deleted. Before the retention period is over the Security Manager can decide to delete a file. As the footage is marked RESTRICTED by ECHA's internal classification, it shall be disposed of accordingly.

3.6 Transfers and disclosure of video material

All transfer and disclosure requests are subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing. This assessment is done by the Security Manager who will enter the request and his decision in a registry. Requests from police authorities (signed by a police officer having a sufficiently high rank), a public prosecutor or a court of law can be considered only if needed to investigate or prosecute criminal offences and when a formal written request is made according to the requirements of the applicable national law regarding form and consent. The disclosure shall only take place if another organisation established under Finnish law would also be required or at least permitted to make the disclosure under similar circumstances. General requests for data mining purposes are explicitly excluded. On official request, the Security Manager can also authorise a police official to see a live replay of video-monitoring material in the ECHA premises without transferring the file.

In exceptional cases, video footage may also be transferred to the European Anti-Fraud Office, the European Ombudsman or the European Data Protection Supervisor on their official request.

On the duly justified request of the investigator appointed by the Authority Authorised to Conclude Contracts (hereafter 'AACC'), video footage may also be transferred for the purpose of an administrative inquiry and the possible follow-up during disciplinary proceedings when the images captured demonstrate a physical security incident or criminal behaviour. Following this procedure the transferred video footage might consequently be disclosed to the investigator, the AACC, the Director of Resources (or the person nominated by the AACC to coordinate the disciplinary procedures), the person assigned by the AACC to hold the hearing, the Disciplinary Board, the Legal Affairs Unit or any other staff member directly involved in the administrative inquiry or disciplinary proceedings.

The Security Manager shall perform a mandatory consultation of the Data Protection Officer of the Agency regarding all transfer requests.

Footage of special categories of data (e.g. of demonstrations) shall not be transferred if there is no clear indication of any criminal offence.

3.7 Process for handling access requests

Any requests by a data subject to receive access to his/her personal data processed via the video-surveillance system shall be addressed to the Security Manager, who will handle the request without undue delay and in line with the ECHA Code of Good Administrative Behaviour, while at the same time safeguarding the rights of third parties present on the same recordings.

If a request is denied, the individual making the request is informed about his/her right to have recourse to the European Data Protection Supervisor.

The same procedure applies when exercising any other right of the data subject.

3.8 Assessment and audit of the system

The Agency's Internal Auditor, with the assistance of the Data Protection Officer, shall perform an adequacy and compliance audit of the video-surveillance system once every two years and also every time a significant change in the circumstances warrants a review. The results shall be summarised in a written audit report.

3.9 Interest group involvement

The opinion of the Staff Committee and the Data Protection Officer of the Agency is sought when major changes are proposed to this procedure.

The Finnish Data Protection Ombudsman is notified of cases where the video-surveillance extends to the Member State's territory.

Simultaneously with adopting this Video-surveillance procedure, the EDPS is notified of the Agency's compliance status by sending them a copy of the Video-surveillance procedure and related documents.

3.10 Informing of the public

Appropriate marking announcing the video-surveillance is in place at the entrance of the ECHA premises.

The video-surveillance policy will be made available to the staff via the Agency's Intranet pages and shall be published on the Agency's internet pages.

In addition, individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- their identity is noted in any files/records,
- the video recording is used against the individual,
- the recording is kept beyond the regular retention period,
- the recording is transferred outside the security unit, or
- the identity of the individual is disclosed to anyone outside the security unit.

Provision of notice may sometimes be delayed temporarily, for example, during an administrative inquiry or if it is necessary for the prevention, investigation, detection and

prosecution of criminal offences. The Agency's DPO is consulted in all such cases to ensure that the individual's rights are respected.

3.11 Confidentiality of information

Everyone granted with an access to the video-monitoring system is informed that all monitoring material is of RESTRICTED security class and owned by ECHA. To this purpose they shall sign a specific confidentiality undertaking, indicating that they shall not record, copy, modify, re-direct or otherwise process the video-stream. Confidentiality obligations apply to the information obtained through the video-surveillance system.

A prior approval of the Security Manager is required before information on footage is revealed to an outsider.

3.12 Training

The Security staff, including the external security guards shall be offered training regarding the proper use of the surveillance system and on Data Protection obligations related to this procedure.

The system administrator and the access control manager will train their back-up persons.

3.13 Recourse to the European Data Protection Supervisor

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 45/2001 have been infringed as a result of the processing of their personal data by the Agency. Before doing so, it is recommended that individuals first try to obtain recourse by contacting:

- The Security Manager at security@echa.europa.eu, and/or
- The Data Protection Officer of the Agency at data-protection-officer@echa.europa.eu.

Staff members may also request a review from their appointing authority under Article 90 of the Staff Regulations.

4. Flowchart

N/A

5. Definitions and acronyms

Term/Abbreviation/Acronym	Definition
AACC	Authority Authorised to Conclude Contracts
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor

6. References

Associated document code	Document name
	Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
	EDPS Video-surveillance Guidelines (issued 17 March 2010)
MB/11/2008 final	ECHA Code of Good Administrative Behaviour