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 the video material produced and recorded by surveillance systems in the ECHA premises and garage.

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.

Description

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

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

Cameras will not monitor areas where 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 of core office hours.

2.1. Coverage

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 R3 Facility and Security Services team 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 higher level of privacy such as leisure areas (canteen, kitchenettes, lounge areas, waiting rooms etc.), toilet facilities, dressing rooms, the gym area, as well as the office of the medical advisor and the office of the staff committee.
- Office areas.

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

2.2. Coverage

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 62.

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 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 features.

Panning, zooming and/or tilting cameras will be used in areas where the monitoring need is so wide and/or deep that otherwise an excessive number of cameras would be required.

2.3. Responsibilities and access rights

The Head of Unit of the Corporate Services 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:

- Those so appointed by the Head of Unit Corporate Services as system owner.

  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(s) is responsible for the access right management;
  - The main administrator(s) has full access to the system;
  - The system owner is responsible for system management issues.

- The external security guards can watch live video; they can pan, tilt and zoom cameras if there is a security or safety related reason to do so.

  The security guards' supervisor will monitor the use of the video-surveillance system and instruct on its proper use. He/she will inform the Facility and Security Services team 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 investigation of a suspected security incident, he/she can be granted with a temporary access to the stored video footage.

The Facility and Security Services team regularly check and validate the users with access to the systems as part of the access management role.

2.4. Storage

The video-surveillance is a standalone system and recordings will 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.

The servers storing the recorded images are located within an access limited secure area of ECHA's premises.

2.5. Retention period

The normal retention period is 28 calendar days (4 weeks). The period has been defined based on the experiences gathered while 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 Head of Unit Corporate Services can decide on a longer retention period on case-by-case basis.

A register is kept by the R3 Facility and Security Services team 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 Head of Unit Corporate Services can decide to delete a file, e.g. peaceful demonstration. As the footage is marked RESTRICTED according to ECHA's Policy on Internal Classification and Handling of Information and Documents, it shall be disposed of in line with the provisions of the aforementioned Policy.

2.6. 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. These assessments will be done by the Facility and Security Services team who will enter the request and it's 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 may only be considered 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 Facility and Security Service team may 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 upon 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 Head of Unit Corporate Services shall perform a mandatory consultation of the Data Protection Officer of the Agency regarding all transfer requests.

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

2.7. Process for handling access requests

Any requests by a person to receive access to his/her personal data processed via the video-surveillance system shall be addressed to the Head of Unit of the Corporate Services, 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.

2.8. 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.

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.

2.9. Informing of the public

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

The video-surveillance procedure 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 Facility and Security Team.

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.

2.10. 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 the property of 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 Head of Unit Corporate Services on the recommendation of the Facility and Security Services team is required before information on footage is revealed to an outsider.

2.11. Training

The Facility and Security Services team, 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 owner, system administrator(s) and the access control manager(s) will ensure back-ups are trained.

2.12. 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 (EU) 2018/1725 or any legal statute that may replace it 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 Officer at physicalsecurity@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.

3. Flowchart

N/A

4. Definitions

Term or abbreviation	Definition
AACC/AIPN	Authority Authorised to Conclude Contracts
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor

6. Records

Record name	Security level	Comments
Specific confidentiality undertakings	Restricted	
Register of transfer requests	Restricted	
Register of video recording material retained after the normal retention period	Restricted	
List of all persons having access to the system	Restricted	

7. References

Associated document code	Document name
n/a	

8. Annexes

N/A