Public

PRIVACY STATEMENT

regarding the processing of personal data related to video surveillance at the ECHA premises

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.

What is the purpose of the collection of personal data?

The personal data shall be processed by ECHA for the purpose of maintaining the security of ECHA, its staff, visitors and other persons as well as protecting the building, assets and information of the Agency. 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.

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.

What is the legal basis for processing your personal data?

The legal basis for the processing can be found in Article 5.1(a) of Regulation (EU) 2018/1725.

What personal data is collected?

The video material produced and recorded by the surveillance systems concerns images of persons and objects captured in live monitoring or stored in video-footage, from which individuals are recognisable in a direct or indirect way, which may include sensitive personal data such as the racial or ethnic origin of the persons. ECHA collects the data of ECHA staff members (including interim and trainee staff), as well as contractors, delegates and visitors entering the ECHA premises including building perimeter grounds 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 (see privacy statement for Organising meetings and events).

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-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 document 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 without 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.

Who has access to your personal data and to whom is it disclosed?

The data collected will only be disclosed to the absolute minimum of persons involved in the process, including:

- 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 ECHA 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.

Who is the data controller?

The Head of Unit of the Corporate Services shall exercise the tasks of the data controller for the purpose of this processing operation.

An external security firm acts as processor. No transfers of personal data to recipients outside the European Economic Area are foreseen.

How long are your personal data kept and how are they protected?

The personal data is kept for 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.

ECHA's 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.

What are your rights?

Any person concerned has the right to be informed about the processing of his/her personal data and is entitled to access and rectify the data collected. Under certain conditions, a right to erasure, restriction, objection and/or data portability also applies.

To exercise the above-mentioned rights, you can contact ECHA via the contact form on ECHA's website. Please use the phrase "Exercising Data Protection rights" in the heading.

However, if you feel your Data Protection rights have been breached you can always file a complaint with ECHA's Data Protection Officer (data-protection-officer@echa.europa.eu) or have recourse to the European Data Protection Supervisor.