Specific Privacy Notice on personal data protection regarding the Video-surveillance -- Closed circuit television (CCTV)

Identity of the Controller

Mr Hans Jahreiss, Head of Administration Department

Fusion for Energy
c/ Josep Pla, nº 2,
Torres Diagonal Litoral, B3
08019 Barcelona, Spain

Purpose of the processing operation

For the safety and security of its buildings, assets, staff and visitors, Fusion for Energy operates a video-surveillance system with the following cameras:

- Four cameras on the ground floor: two in the reception desk and one for each of the two external doors (doors for providers directly accessible from the street).
- One camera on each of the lifts halls of F4E floors: 2nd, 7th, 8th, 9th, 10th, 11th, 12th, 13th
- One camera for the ITroom on the 7th floor
- One camera for the ITroom on the 2nd floor.

The purpose of this surveillance is only detecting, deterring and preventing all kind of attacks, illegal access or other incidents (e.g. theft, vandalism, flood, fire).

The processing will be done through dome network cameras HIKVISION connected to a software of the company AEOS.

The system is not used for any other purpose, such as for example to monitor either the work of employees or to monitor presence of staff or contractors. Nor is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access).

Legal Basis

Council Decision of 27 March 2007 “establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it” - 2007/198/Euratom, as last amended by Council Decision of 10th February 2015 (2015/224 Euratom), O.J. L 37, 13.2.2015, p. 8, in particular Article 6 thereof;

Statutes annexed to the Council Decision (Euratom) No 198/2007 "establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it", as last amended on 10th February 2015, in particular Article 10 thereof ;

Staff Regulations of Officials (SR) and Conditions of Employment of Other Servants of the European Communities (CEOS), in particular Article 1e (2) SR.

Lawfulness of the processing

Processing is necessary for the performance of F4E tasks on the basis of the F4E founding instrument or other legal instrument adopted on the basis thereof or in the legitimate exercise of official authority vested in F4E or in a third party to whom the data are disclosed (Regulation (EC) 45/2001, Article 5(a).

Data Subject(s) concerned

The data subjects will be all the individuals entering at F4E's reception desk (e.g. F4E staff, external staff, visitors), at the common lift areas on the floors 2, 7, 8, 9, 10, 11, 12 and 13. and in the IT rooms of the 2nd and 7th floor. Or through the external doors on the ground floor.

Categories of data

The video-surveillance system makes use of conventional systems which record digital images with indication of time, date and camera number.

The cameras operate continuously during 24 hours a day, from Monday to Sunday.

The CCTV does not interconnect its system with other systems, and it does not use covert surveillance, sound recording, or "talking CCTV".

Recipients of the data processed

Recorded video-surveillance material is accessible to Head of Corporate Services Unit, Security Officer, Security Officer's back up and the Security guards. For technical reasons, if necessary, the responsible ICT person may also have access to the material.

The images are additionally accessible to an identified external technical support person from AEOS needed for the maintenance of the functioning of this system.

Date when processing starts

March 2016

Time limits for Storage/ Retention period

The video-surveillance material will be stored in the storage system for 7 days, and will be automatically deleted after this period.

(When cameras are installed for purposes of security and access control, one week should be, in principle, more than sufficient for security personnel to make an informed decision whether to retain any footage for a longer period in order to further investigate a security incident or use it as evidence.)

Rights of the data subject

(Rights of access, to rectify, to block, to erase, to object, according to Article 13-20 of Regulation 45/2001)

Right of access:

Data subjects have the right of access to the personal data that are processed by F4E, specifically:

- if data related to him/ her are being processed
- information on the purposes of the processing operation
- categories of data concerned
- recipients or categories of recipients to whom the data are disclosed
- communication in an intelligible form of the data undergoing processing and their source
- logics involved in any automated decision process concerning him/her

Data subjects shall always have their right of access granted to control if the data reflect the facts and perceptions that they wanted to transmit and if their statements are as complete and accurate as possible.

Right of rectification:

They also have the right to modify any inaccurate or incomplete administrative data, without delay.

Right of blocking:

Data subjects have also the right to obtain from Data Controller blocking of their personal data when:

- they contest the accuracy of the data;
- the controller no longer needs them but they need to be maintained for purposes of proof;
- the processing is unlawful and the data subject requests blocking instead of erasure.

Personal data blocked shall only be processed for the purpose of proof (with the consent of the data subject) or for the protection of the rights of a third party.

Right of erasure:

Data subjects can request the cancellation of their personal data if they consider that they are subject to an unlawful processing.

Right to object:

according to Article 18 of Regulation 45/2001, the data subjects can object the processing of their personal data unless the processing is needed for the purposes of Article 5b) and d) of Regulation 45/2001:

- on legitimate grounds relating to their particular situation
- before their personal data are disclosed to third parties.

Limitations:

However, the Controller may restrict access to the information/documents to safeguard:

- the prevention, investigation, detection and prosecution of criminal offences
- any important financial or economic interest of the Member States
- the protection of the data subject or the rights of freedoms of others
- the national security, public security or defence of the Member States
- the monitoring, inspection or regulatory task connected with the exercise of official authority.

Common steps for the exercise of any of the above mentioned rights:

Any request from a data subject concerning the rights above described should be addressed to the Controller through the following contact e-mail address: Resources-Controller@f4e.europa.eu.

Apart from the right to obtain the rectification without delay (Art. 14), the Controller shall provide an answer to the data subject concerning his/her request on the exercise of his/her rights, as defined above, within 10 working days. Any contestation by the data subject to the Controller's reply shall be submitted within 10 working days of the response received and the Controller shall have another 10 working days to provide a replica revising his previous decision or confirming it.

The data subject may put in place the procedure established in article 90 of the Staff Regulations to contest any action of the data controller related to his/her rights.

If you feel your Data Protection rights have been breached you can file a complaint with the F4E's Data Protection Officer DataProtectionOfficer@f4e.europa.eu or have recourse at any time to the European Data Protection Supervisor: EDPS@edps.europa.eu. The EDPS receives complaints from EU staff members as well as from other people who feel that their personal data have been mishandled by a European institution or body.