Information notice concerning video surveillance in the buildings of the Court of Justice of the European Union

This notice provides (1) information on the general video-surveillance system put into place by the Institution and (2) information concerning the possibility of having recourse to a device designed for the purpose.

1. Information on video-surveillance in general

The Institution has put into place a video-surveillance system to ensure the general security of persons and property in accordance with the Blueprint for ensuring the safety of the building complex of the Court of Justice of the European Union. The purposes and manner of processing the images filmed are set out in detail in a document entitled 'Video-surveillance Policy' which may be accessed on the internet site of the Institution and on the intranet sites of the Security and Safety Section and the Data Protection Officer.

Surveillance cameras are positioned on the exterior and in the interior of the buildings of the Institution (random or directed selection of the locations filmed).

Images of the persons concerned (persons entering the buildings of the Institution or outside near to the buildings) are the only data collected by the system.

The person responsible for the processing of data is the Head of the Security Service, tel +352 4303-1, securite@curia.europa.eu.

The images are recorded and used in accordance with:

- 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,
- the recommendations of the European Data Protection Supervisor ('EDPS') set out in the Video-surveillance Guidelines of 17 March 2010. [1]

The images are processed for the following purposes:

[1] The Video-surveillance Guidelines are available on the internet site of the EDPS: https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Supervision/Guidelines

- Access and security controls (security of persons, buildings, property and information);
- Determining the source of a fire, estimating its effect with a view to possible evacuation of a building, monitoring emergency exits;
- Monitoring works of art;
- Deterrence (damage to the property of the institution, assaults on persons);
- Finding those responsible for any offences.

The images recorded are kept for a maximum of 30 days but, in the event of suspicion and/or discovery of an offence, the relevant data are kept for the duration of any inquiry and proceedings (e.g. disciplinary or criminal) which may follow. Acess to the images recorded is restricted to a limited number of persons and all technical and physical measures are in place to avoid inappropriate use thereof.

The following persons have access to the images:

- Officials and agents of the Security Service of the Buildings Directorate (viewing, recording, copying, archiving, deletion);
- Employees of the security firm who perform in part security functions (viewing in real time without access to the recorded images).

The images may be communicated to other addressees in particular situations:

- The Court of Justice ('Court'), the General Court ('General Court') and/or the Civil Service Tribunal ('CST') or a national court, and to the lawyers and Agents of parties if there is a dispute;
- The formation of the Court, General Court or CST responsible for examining claims, the President and Registrar of the court concerned and the Legal Advisor for administrative matters, in the event of a claim brought under Article 90(2) of the Staff Regulations of Officials;
- Persons called upon to perform duties in the context of an administrative inquiry ordered by the Appointing Authority or the Authority empowered to conclude contracts of employment or in disciplinary proceedings commenced, in accordance with the rules laid down in Annex IX to the Staff Regulations of Officials of the EU, following a security incident;
- The President and Registrar of the Court together with the officials who may assist them, under the responsibilities devolved to them by Article 20(4) of the Rules of Procedure of the Court;
- The EDPS in accordance with Article 47(2) of Regulation No 45/2001;
- The Data Protection Officer of the Institution in accordance with point 4 of the Annex to Regulation No 45/2001;
- The European Ombudsman, in so far as necessary for dealing with a complaint made to him (Article 228 TFEU);
- OLAF in the event of an inquiry under Regulation No 883/2013 and the Decision of the Court of Justice of 12 July 2011 concerning the terms and conditions for internal

investigations in relation to the prevention of fraud, corruption and any other illegal activity detrimental to the interests of the European Union.

Finally, under the conditions laid down in Article 8 of Regulation No 45/2001, images may be transferred to national authorities if that proves necessary for the purposes of an inquiry carried out in the exercise of their powers.

All transfers of data are recorded in a specific register.

Any person who wishes to obtain additional information or exercise his/her rights under Regulation No 45/2001 (access, rectification, blocking, erasure or objection) may apply to the Head of the Security Service.

Articles 13 and 14 of Regulation No 45/2001 concerning the right of access and the right to rectification respectively, are cited in full below.

Any person whose personal data are processed can also apply to the EDPS pursuant to Article 32(2) of Regulation No 45/2001.

Article 13 of Regulation No 45/2001

Right of access

The data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller:

(a) confirmation as to whether or not data related to him or her are being processed;

(b) information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

(c) communication in an intelligible form of the data undergoing processing and of any available information as to their source;

(d) knowledge of the logic involved in any automated decision process concerning him or her.

Article 14 of Regulation No 45/2001

Rectification

The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

2. Information concerning covert video surveillance (Chapter 4.4 of the Video-surveillance policy of the Court of Justice of the European Union, 'Covert video surveillance')

The general video-surveillance system does not include any covert video-surveillance equipment.

In the context of an internal security investigation, on the basis of an impact analysis (submitted to the Data Protection Officer for opinion) and after a decision of the Registrar of the Court, the institution may, exceptionally, use a covert video-surveillance system, separate and not connected to the general video-surveillance system, to identify repeat intruders, thefts and other serious infringements of the security regulations.

The impact analysis must clearly show how the undermining of privacy and protection of personal data resulting from the use of a covert video-surveillance system is outweighed by the advantages obtained from the use of that system.
To that end, that analysis takes into account, in addition to the guarantees surrounding the use of the general video-surveillance system, a series of criteria, including the lack of alternative measures having less impact on privacy and the restrictions placed on the use of the proposed equipment (location, times and period of use of the equipment, the choice of which is itself determined on the basis of the offences discovered).

The covert video-surveillance equipment may not, in any situation, be connected to the general video-surveillance system. Accordingly, the images recorded are collected manually.
Those images are viewed as soon as possible and at the latest within seven working days of their recording in order to evaluate their relevance. That maximum period of seven days is necessary in so far as daily operations on the equipment could adversely affect the progress of the internal security investigation, but also in order to have sufficient time to carry out the manual collection of the images from that equipment.

Images which are not relevant to the internal security investigation are immediately erased after their first viewing.
Images relevant to the internal security investigation are kept until that investigation and any proceedings arising therefrom are closed.

The persons identified on the images are individually informed by the Security and Safety Section if at least one of the following conditions is satisfied:

- the person’s identity has been noted in a file;
- the video recording is used against the person;
- the video recording is kept beyond the periods set out above;
- the video recording is transferred outside the Security and Safety Section; or
- the person’s identity is communicated to a person outside the Security and Safety Section.

Provision of that information may be deferred if that is necessary for the purposes of the internal security investigation or in other situations provided for in Article 20 of Regulation No 45/2001 (cited in full below).

Article 20 of Regulation No 45/2001

Exemptions and restrictions

1. The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 and Article 37(1) where such restriction constitutes a necessary measure to safeguard:

(a) the prevention, investigation, detection and prosecution of criminal offences;

(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;

(c) the protection of the data subject or of the rights and freedoms of others;

(d) the national security, public security or defence of the Member States;

(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).

2. Articles 13 to 16 shall not apply when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that there is clearly no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.

3. If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor.

4. If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

5. Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect.