Directorate-General for Infrastructure

Video-surveillance policy

Court of Justice of the European Union

TABLE OF CONTENTS

1. Objective and scope of the video-surveillance policy of the institution

On 5 July 2005, the 'Buildings' Committee of the Court of Justice of the European Union took note of the *Blueprint for the overall safety of the buildings complex of the Court of Justice of the European Communities*.

The various recommendations in that study included the installation of a video-surveillance system in order to ensure the security of the buildings, assets and persons.

Accordingly, the institution has put in place a video-surveillance system. A report on the progress of the use of the video-surveillance system was presented to the Administrative Committee, which took note of it at its meeting on 1 July 2009.

This document describes the current video-surveillance system and the measures taken by the institution to protect personal data, privacy and the other fundamental rights.

2. Privacy, data protection and the conformity of the video-surveillance system

2.1 Revision of the existing system

The Court of Justice of the European Union was operating a video-surveillance system before the Video-Surveillance Guidelines (the 'Guidelines') of 17 March 2010 issued by the European Data Protection Supervisor ('the EDPS') were published.

The video-surveillance system and the institution's procedures were brought into line with the legislation on the protection of personal data and, more particularly, with the recommendations of the EDPS set out in the Guidelines. [1]

2.2 Compliance status

The Court of Justice of the European Union handles the images in compliance 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 ('Regulation No 45/2001') and the Guidelines.

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

2.3 Internal audit

An internal audit shall be carried out every 2 years.

2.4 Information on the compliance status to the EDPS

The EDPS was notified of the handling of personal data inherent to the video-surveillance system for the first time in April 2009.
Following the adoption of this video-surveillance policy, the Court of Justice of the European Union has notified the EDPS of the compliance status by sending him a copy of this document.

2.5 Contact with the Member State authority responsible for data protection

The authority responsible for data protection in Luxembourg (Commission nationale pour la protection des données - CNPD) was informed in November 2006. Its comments and recommendations [2] have been taken into account.

2.6 Transparency

The video-surveillance policy is available:

- on the internet site of the intranet of the Safety and Security Section: http://intranet/infrastructures/indispensables/securite.htm
- on the internet site of the Data Protection Officer: http://intranet/dpo/FR/Home_FR.htm
- On the website of the Court of Justice of the European Union at the following address:
- http://curia.europa.eu/jcms/jcms/P_127468: The institution > Getting to the Court > General conditions.

2.7 Periodic checks

Every two years, the Safety and Security Section of the institution will carry out a check concerning data protection. At the time of those periodic checks, an analysis will be made of:

- the need for a video-surveillance system;
- the suitability of the system to meet the objectives laid down;
- the lack of adequate alternatives.

[2] In particular in a letter of 15/03/2014 addressed to the person responsible for data handling, the CNPD stated that '*only Regulation No 45/2001 will apply, since the video-surveillance system … will be limited strictly to the private domain, excluding any surveillance of the public domain'.*

The periodic checks are intended in particular to ascertain whether the video-surveillance policy of the Court of Justice of the European Union remains in line with Regulation No 45/2001 and the Guidelines (suitability audit) and whether that policy is followed in practice (compliance audit).

2.8 Technical solutions favouring privacy

The Court of Justice of the European Union has implemented the following technological solutions which respect privacy:

- The viewpoints and the camera lenses have been chosen to cover only the areas to be monitored;
- The areas of the buildings where the expectation of privacy is even higher are not monitored by cameras;
- Specific software, a user profile and a password are required for the persons authorised, that is to say a small number of members of the Security and Safety Section, to access the images recorded;
- All activity on the system is recorded (recording of the activity and the relevant active user).

3. Locations under surveillance

In accordance with the Security blueprint, a video-surveillance system of 526 cameras has been installed on the current site (surface of around 220 000 m²).

The video-surveillance system covers:

- External surfaces/Emergency exits
  Objective: to deter any attempt to gain access and to deter offensive behaviour

- Access to the various buildings' reception
  Objective: to monitor the flow of entries and exits

- Access to the car parks (barriers and gates)/Ramps and traffic routes in the various levels of the car parks
  Objective: to deter any damage to the institution's assets or assaults on persons and to assist in the resolution of disputes in that regard

- Delivery platforms and equipment storage floor
  Objective: to monitor deliveries and the access to the delivery platforms and the equipment storage floor, protection of sensitive technical installations

- Public areas inside the buildings

  Objective: to enable the Command and Security Post to have an overview of the general situation so that it may react to any incident (disorderly conduct, a suspect abandoned package, a person suffering a fall, etc); surveillance of the works of art; rapid intervention in the event of fire or illness

- Passages to private protected areas

  Objective: to prevent any attempt to gain unlawful access to those areas and, via the intercom system, to assist users as necessary with difficulties connected with the access control equipment (access gates or badge readers)

Plans showing the siting of the cameras are available from the Security and Safety section of the institution and may be consulted there. Those plans are available, on request, to the Data Controller, the Data Protection Officer of the institution ('the DPO') and the EDPS.

No cameras cover locations where persons may expect greater respect for their privacy.

4. Personal information collected and the reason for its collection

4.1 Brief description and detailed technical specifications of the system

The video-surveillance system records digital images and is equipped with a movement detection system. The system records movements detected by the cameras in the surveillance areas and the date, time and location. The cameras function 24 hours a day, 7 days a week. The image quality, depending on the siting, can enable persons to be identified. The majority of the cameras are fixed. Some cameras have a limited power optical zoom making it possible to zoom in on a location or a person to follow him/her if necessary.

The video-surveillance system does not use so-called intelligent technologies, is not connected to other systems, does not use covert surveillance, does not record sound signals and does not use 'speech-enabled surveillance cameras'.

4.2 Objective of the surveillance

The institution uses its video-surveillance system exclusively to monitor access and security (the security of persons, buildings and information).
Those installations supplement the access control systems, the emergency exit management systems and the fire safety systems.

The video-surveillance system forms part of the group of measures put in place to strengthen the general security policy and helps to prevent, deter and, if necessary, investigate any unlawful access (high-risk locations, IT infrastructures and operational information).
In addition, video surveillance helps to prevent, detect and investigate thefts of equipment or property belonging to the institution, its staff or visitors. Video surveillance also contributes to ensuring the safety of the users of the buildings (for example, in the event of fire, assault, etc.).

4.3 Limitation of scope

Video surveillance is used solely for the purposes set out above. The video-surveillance system is not used to assess the work of staff or to check their presence.
The system is used as an aid to investigation only in the event of a security incident (thefts, unauthorised access, etc.) and, exceptionally, images may be transferred to other official bodies in the exercise of their powers and duties (judicial or disciplinary enquiries, OLAF investigations, etc.). Those transfers are described in Chapter *6.5 Transfers and disclosure* below.

4.4 Covert surveillance

There is no provision for covert surveillance operation as part of the video-surveillance system. Nevertheless, in rare cases and without any connection to the general video-surveillance system, the institution may use covert video-surveillance equipment.

That equipment can be used only under the following conditions:

- to identify repeat intruders, thefts or other serious infringements of the security regulations,
- for a strictly limited period,
- in precisely defined locations,
- on the basis of an impact assessment submitted for opinion to the institution's Data Protection Officer,
- and following a decision of the Registrar of the Court of Justice of the European Union.

The period of use of the covert video-surveillance equipment shall not exceed the period over which the incidents which led to its use occurred. The equipment shall, moreover, be removed immediately upon identification of the person(s) responsible.

The siting of covert video-surveillance equipment shall be defined on the basis of the location of the incidents which led to its use. It cannot be sited in areas where privacy is naturally to be expected (sanitary installations).

The placing of covert cameras is subject to stringent conditions, of which the EDPS is informed for the purpose of a prior check and which ensure that the effect on privacy is kept to a minimum.

4.5 Webcams

There are no webcams connected to the video-surveillance system of the Court of Justice of the European Union.

4.6 Collection of special categories of data

No data in the special categories of data referred to in Article 10 of 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 [3] is collected.

If demonstrations were to be held outside the buildings of the Court of Justice of the European Union, the following additional guarantees are in place:

- Demonstrations are monitored only for security reasons;
- The cameras cannot be fixed on faces and must not attempt to identify persons, save in the event of an imminent threat to public safety or violent criminal behaviour (vandalism, attacks);
- The images cannot be used for data-mining purposes; [3]
- All those who operate the video installations shall receive training (see point *6.3 Data protection training* below) to avoid any disproportionate effect on the privacy and other fundamental rights of the participants filmed, including their freedom of assembly.

5. Legitimacy and legal basis of the video-surveillance system

Use of the video-surveillance system for security and access control purposes is necessary to ensure the smooth running of the institution and the legitimate exercise of the official authority vested in it.

[3] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life.

The use of the video-surveillance system, as it is operated by the Court of Justice of the European Union, complies with Article 5(a) of Regulation No 45/2001.

This video-surveillance policy, which forms part of a wider series of security policies adopted by the institution, provides a more detailed and specific legal basis for video surveillance.

6. Access to the information and data collected

6.1 Security and Safety Section of the institution and the security firm

Security guards from a security firm are responsible for viewing the real-time images transmitted. [4]
It is not possible for the security guards from the security firm to access the recorded images.

The specifications annexed to the services contract concluded with the security firm contain a confidentiality clause and an article on data protection to ensure that the security guards uphold the protection of personal information. Those specifications also include a specific reference to video surveillance (see Annexes 1a and 1b).

The recorded images are accessible only to the staff of the Security and Safety Section of the institution.
All members of the Security and Safety Section are required to sign a statement of confidentiality concerning the use of the video-surveillance system.

6.2 Access rights

The 'Internal video-surveillance procedure' [5] states clearly who has access to the recorded images and to the technical installations of the video-surveillance system, on what conditions and with what access rights.

Specific software, a user profile and a password are necessary to have access to the images recorded. That specific software is installed on the computers of only certain members of the institution's Security and Safety Section.

[4] That security firm is a processor for the purposes of Article 2(e) of Regulation No 45/2001. That security firm processes personal data in accordance with the requirements laid down in Article 23 of Regulation No 45/2001.

[5] The Internal video-surveillance procedure is an internal document, which specifies who is authorised to view the real-time images, view the recorded images, copy the images, make a download, erase and process recorded images.

6.3 Data protection training

All staff holding access rights, including the security guards from the security firm, have received training on data protection.
New members of the security staff receive training systematically when they join the service.
Workshops on compliance with the data protection rules are organised every two years for staff holding access rights.

6.4 The security staff confidentiality undertaking

Each member of the Security and Safety Section of the institution who has the right to process images has signed a confidentiality undertaking after undergoing data protection training.
Each member of staff of the security firm who has the right to process images has signed a confidentiality undertaking after undergoing data protection training.

6.5 Transfers and disclosure

No transfer or disclosure of data shall be made except by the Data Controller, namely the Head of the Security and Safety Section, after consulting the DPO.
Any transfer or disclosure of data to addresses external to the Security and Safety Section shall be subject to a thorough assessment as regards the need and compatibility of its purpose with the purpose initially pursued, namely security and access control.

Such transfers shall be systematically recorded in the retention and transfer register held by the Head of the Security and Safety Section.

The Human Resources and Personnel Administration Directorate has no right of access to the data processed.

On the conditions defined in Article 8 of Regulation No 45/2001, images may be transmitted to the Luxembourg police if that proves necessary for the purposes of an inquiry carried out in the course of their duties. Where there is doubt, the Security and Safety Section shall consult the Legal Advisor for administrative matters.

Images may also be transmitted in exceptional circumstances to:

- The Court of Justice (Court), the 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;

- 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;
- 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 DPO 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).

7. Data and information protection measures

The principal technical and organisational measures put into place to protect the security of the video-surveillance system, including personal data, are as follows:

- The servers on which the images are recorded are sited in secure locations, protected by physical security measures; firewalls are installed to protect the IT installations;
- Each member of the security staff (internal and external) has signed a confidentiality undertaking;
- User access rights to the video-surveillance system are restricted to the tools necessary to carry out their work;
- Only the system manager, designated by the Data Controller, is authorised to grant, modify or cancel user access rights. The grant, modification or cancellation of access rights is carried out in accordance with the criteria laid down in the Internal video-surveillance procedure;
- The Internal video-surveillance procedure shall contain an up-to-date list of the persons who have access to the system, in which the extent of their access rights is specified.

8. Retention of data

The images are retained for a maximum of 30 days.
After 30 days, the recordings are automatically erased.
That period is justified by:

- Current experience that security incidents are often reported to the Security and Safety Section of the institution more than two weeks after they occur;
- The practice of criminals/terrorists of reconnoitring the buildings before committing an unlawful act;
- The high number of visitors amounting to approximately 100 000 persons per year.

Certain images may be retained for a longer period if that retention is necessary for the purposes of an inquiry or to serve as evidence related to a security incident. That retention is documented (electronic register) and the reasons for retaining the images for more than 30 days are stated. A paper copy of the retention and transfer register is to be found in Annexes 2a and 2b. The need for that retention shall be regularly re-assessed.

The video surveillance is monitored in real-time by the security guards in the Safety and Fire Command Post (SFCP), 24 hours a day, 7 days a week.

9. Public information and specific individual information

9.1 Information via various media

Appropriate and full information on video surveillance shall be made available to the public. That information shall be provided via the following media:

- Warning signs are placed at the various access points to the buildings. Those signs shall advise of the presence of a video-surveillance system and state in particular the length of time for which images are retained and the contact details of the service responsible;
- A notice giving the information required under Article 12 of Regulation No 45/2001 is available at the reception of each building, on the intranet sites of the Security and Safety Section and of the DPO and on the website of the institution (http://curia.europa.eu/jcms/jcms/P_127468: The institution > Visiting the Court > General conditions). That notice gives a telephone number and an email address in order to enable persons interested to obtain additional information;
- This Video-surveillance policy is accessible on the intranet sites of the Security and Safety Section and of the DPO and on the internet site of the Court of Justice of the European Union (cf. point 2.6 Transparency).

Copies of the warning signs and the information notice are attached in Annexes 3a and 3b.

9.2 Specific individual notification

When persons are identified on the images (for example, for a security investigation), they must be informed of that fact individually if at least one of the following conditions is satisfied:

- Their identity is noted in a file;
- The video sequence is used against the person in question;
- The video sequence is retained for a period longer than the period prescribed;
- The video sequence is transferred outside the Security and Safety Section;
- The identity of the person is communicated to persons outside the Security and Safety Section.

Provision of that individual information may be delayed, in accordance with Article 20(1)(a) of Regulation No 45/2001, if that is necessary to ensure the prevention, investigation, detection or prosecution of criminal offences. The DPO shall be consulted in the event that the application of this restriction is envisaged.

10. Rights of the data subjects

Persons filmed have the right of access to personal data concerning them and to have those data rectified if they are inaccurate or incomplete.

As regards exercise of the right of access, it is possible to organise a viewing of the images or to provide the requesting party with a copy of the images recorded. In that case, the requesting party must show identification before viewing the images. S/he must also state the date, time, location and circumstances in which s/he was filmed.

Currently, requesting parties may view the images free of charge and, if the data subject can show a legitimate interest, obtain a copy of them also free of charge. The principle that such services are provided free of charge may be reviewed in the event that the number of applications rises significantly.

On the conditions laid down in Articles 15 and 16 of Regulation No 45/2001, the data subjects can also have the personal data concerning them blocked or erased. In the event of a request for erasure, the Data Controller shall consult the DPO.

The rights of the data subjects may be restricted in accordance with Article 20(1)(a) of Regulation No 45/2001 if that is necessary to ensure the prevention, investigation, detection and prosecution of criminal offences.

The rights of the data subjects may also be restricted in accordance with Article 20(1)(c) of Regulation No 45/2001 if that proves necessary to ensure the protection of the data subject or the rights and freedoms of other persons.
For example, if a data subject wishes to have access to the clips in which s/he appears, it may be necessary to restrict his/her right of access in the event that another person also appears in the same clip and that person's consent has not been obtained, in so far as the video-surveillance system currently used does not enable the image of a person to be masked.

The Data Controller shall consult the DPO where it is proposed to apply a restriction to the rights of data subjects.

All requests for access, rectification, blocking or erasure must be addressed to:

Head of the Security and Safety Section, Data Controller
Court of Justice of the European Union
L-2925 Luxembourg
Tel: +352 4303-1
securite@curia.europa.eu

The Security and Safety Section can also be contacted for any other question concerning the processing of personal data as regards the video-surveillance system put into place in the Court.

If possible, the Security and Safety Section will respond to all requests within 15 working days. If it is not possible to meet that deadline, the requesting party will be informed within 15 days of the progress of his/her request and of the reasons why it was not possible to deal with it within the period prescribed. In all cases a response must be provided within three months at the latest.

11. Right of action

Pursuant to Article 32(2) of Regulation No 45/2001, without prejudice to any judicial remedy, any data subject may submit a claim to the EDPS (edps@edps.europa.eu) if s/he believes that his/her rights under Article 16 of the Treaty on the Functioning of the European Union have been infringed following the processing of personal data by the institution.

Before making such a claim, the data subjects are requested to attempt to resolve the matter by contacting:

the **Head of the Security and Safety Section, Data Controller**
Court of Justice of the European Union
L-2925 Luxembourg
Tel.: +352 4303-1
securite@curia.europa.eu

and/or

the **Data Protection Officer**
Court of Justice of the European Union
L-2925 Luxembourg
tel: +352 4303-1
DataProtectionOfficer@curia.europa.eu

The members of staff, in accordance with Article 90 of the Staff Regulations of Officials, may request an examination by the Appointing Authority/the Authority empowered to conclude employment contracts.

Annexes

Annex 1a	*Extract of Article 16 of Contract CJ 03/2010 concerning data protection*
Annex 1b:	*Extract of the specifications for call for tenders CJ 03/2010 on the video-surveillance system*
Annex 2a :	*Register of recordings retained*
Annex 2b :	*Register of transfers and disclosures*
Annex 3a:	*Warning signs*
Annex 3b:	*Information notice*

Annex 1a to the Video-surveillance policy

Article 16 – Data protection

1. Data processed by the Court of Justice of the European Union

   a. The Court of Justice of the European Union shall process personal data 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.

   b. Those data shall be processed exclusively for the purposes of the performance, management and monitoring of the contract by the Buildings and Security Unit and the Budget and Accounts Department, without prejudice to any transmission of those data to the bodies carrying out monitoring or inspections in accordance with EU law.

   c. If the contractor were to find itself in one of the situations of exclusion referred to in Articles 93 and 94 of the Financial Regulation (Council Regulation No 1605/2002 of 25 June 2002), data concerning it shall be recorded in the database provided for in Article 95 of that regulation and may be communicated by the Commission to persons authorised to receive them, designated by the other institutions, agencies, authorities or bodies referred to in that article by application of Article 134a(2) of Regulation No 2342/2002 laying down detailed rules for the implementation of the Financial Regulation, as amended, and Commission Regulation (EC, Euratom) No 1302/2008 of 17 December 2008 on the central exclusion database.

   d. In the context of performance of a contract, the following categories of data may also be processed: name, address, telephone and fax numbers, e-mail address;

   ➔ Data contained in the passport or certificate of nationality (copy);
   ➔ Proof of self-employed status, proof of taxable status;
   ➔ Banking data (account number, bank name, IBAN code);
   ➔ Data contained in an extract from the judicial record, a certificate attesting to (non) payment of social security contributions or tax;
   ➔ Curriculum vitae;
   ➔ List of the main publications or achievements;
   ➔ Declaration of the turnover of the tenderer;
   ➔ Bank declaration or proof of professional indemnity insurance;
   ➔ Other data related to the contractor, transmitted by it in performance of the contract.

Furthermore, personal data are generated by the persons participating in the contract performance assessment (in particular assessment data).

e. Recipients may also include the Court of Auditors, the specialised financial irregularities committee, the internal auditor (within the responsibilities conferred on him by Articles 85 to 87 of the Financial Regulation), the European Parliament (under the discharge procedure), OLAF, the Supervisory Committee of OLAF (pursuant to Article 11 of Regulation No 1073/1999), the General Court of the European Union and the Court of Justice of the European Union, the courts or tribunals having jurisdiction (as a general rule, the Luxembourg courts) in the event of legal proceedings relating to performance of the contract, the President and the Registrar of the Court together with the officials who may assist them, under the responsibilities devolved to them by Article 23 of the Rules of Procedure of the Court, and the legal adviser in respect of administration.

f. Under Article 49 of Regulation No 2342/2002, documents relating to the contract and containing personal data shall be kept for five years from the date on which the Parliament grants discharge for the budgetary year in the course of which performance of the contract is completed or in the course of which the contractually agreed or statutory warranty which the contracting authority may enjoy under the contract expires. Personal data contained in supporting document shall be deleted where possible when those data are not necessary for control and audit purposes.

g. The contractor and persons in respect of whom personal data is processed in relation to the performance of this contract may, on request, obtain the communication of their personal data and rectification of any inaccurate or incomplete data. They are requested to put any question concerning the processing of those data to the Head of the Buildings and Security Unit. They also have the right to apply at any time to the European Data Protection Supervisor.

h. The representative(s) of the contractor is/are bound to inform the persons to whom personal data used in connection with the present contract of the type, purpose and characteristics of that processing (categories of data, addressees, retention period, etc.) and of the rights set out above.

2. <u>Data processed on behalf of the Court of Justice of the European Union</u>

a. The contractor shall act on the instructions of the Data Controller.

b. It shall comply with the applicable rules relating to the protection of personal data.

c. With regard to data confidentiality and security, the contractor shall also be subject to the obligations referred to in Articles 21 and 22 of Regulation (EC) No 45/2001 unless, by virtue of Article 16 or the second indent of Article 17(3) of Directive 95/46/EC, the contractor is already subject to obligations of confidentiality and security set out in the national legislation of one of the Member States.

Annex 1b to the Video-surveillance policy

7.2.3. Access control and anti-intruder detection system

The Court of Justice shall make available to the Contractor a centralised system installed throughout the site enabling access control and intruder detection. The GSC tool will be applied for its use in real time. None the less, in reduced mode, the guard on duty at the SCP will be able to use the native subsystem.
The visitor management module is operated by the guards and receptionists at the reception desks.

7.2.4. Video-surveillance system

7.2.4.1. General

The Court of Justice shall make available to the Contractor the fully digital system, constituting the following equipment and subsystems:

➔ Fixed and mobile video-surveillance cameras;

➔ High storage capacity digital recorders with mastering function and automatic continuous pre and post alarm fixed image record function;

➔ Interior and exterior video detection system (automatic motion detection within the camera field).

Fixed cameras shall be used to monitor the main access control obstacles and sensitive areas.

Fixed cameras with video detection shall be used to monitor the exterior of the buildings, supplemented by mobile cameras for additional security.

The GSC tool will be applied for the use in real time of the video-surveillance system. None the less, in reduced mode, the guard on duty at the SCP will be able to use the native subsystem.

7.2.4.2. Respect for privacy – data protection

The Contractor shall act on the instructions of the Data Controller. It shall comply with the applicable rules on the protection of personal data and, in particular, 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 and, more particularly, the provisions on data confidentiality and security (Articles 21 and 22 of the regulation);

➔ the European Data Protection Supervisor's (EDPS) Video-surveillance Guidelines;

➔ the Video-surveillance policy of the Court of Justice;

➔ the instructions given by the Court of Justice;

➔ the recommendations of the European Data Protection Supervisor (EDPS) or the Data Protection Officer of the Court of Justice in the exercise of their control/inspection or consultation duties.

The Contractor undertakes to provide appropriate training to the staff operating the cameras, relating in particular to the obligations as regards data protection and the European Data Protection Supervisor's (EDPS) Video-surveillance Guidelines.

Annex 2a - REGISTER OF RECORDINGS RETAINED (in accordance with point 7.2 of the Guidelines)

No	Incident date	Time		Camera		Incident description	Reason for retention	Expected date of review	Recording name
		Start	End	Number	Location				

Annex 2b - REGISTER OF TRANSFERS AND DISCLOSURES (in accordance with point 10.5 of the Guidelines)

Number	Incident date	Identification of requesting party				Person authorising transfer			Brief description of recorded content	Reason for request and for authorisation	Transfer	Disclosed	If verbal information given, state type of information
		Surname	Given name	Post	Service	Surname	Given name	Post					

Annex 3a - Warning signs

VIDÉOSURVEILLANCE

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance.

Les images sont conservées pendant 30 jours.

Pour de plus amples informations, veuillez consulter la page http://curia.europa.eu/jcms/jcms/P_127468 ou prendre contact avec la section sécurité en téléphonant au +352 43031ou en adressant un courriel à securite@curia.europa.eu

VIDEOÜBERWACHUNG

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht.

Die Aufnahmen werden 30 Tage lang gespeichert.

Weitere Auskünfte erhalten Sie unter der adresse http://curia.europa.eu/jcms/jcms/P_127468 Sie Können sich aber auch mit der Sicherheitsabteilung unter +352 43031 oder securite@curia.europa.eu in Verbindung setzen

VIDEO SURVEILLANCE

For your safety and security, this building and its immediate vicinty are under video-surveillance.

Recording are retained for 30 days.

For further information, please consult http://curia.europa.eu/jcms/jcms/P_127468 or contact the security section at +352 43031 or securite@curia.europa.eu

Annex 3b – Information notice

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.