Rules governing the use of Video-surveillance within the SESAR Joint Undertaking

Public Version

Update No.2

1 PURPOSE AND SCOPE OF THE SESAR JOINT UNDERTAKING'S VIDEO-SURVEILLANCE POLICY

For the safety and security of its buildings, assets, staff and visitors, the SESAR Joint Undertaking (hereinafter referred to as the "SJU") operates a video-surveillance system. The present rules related to SJU Video-surveillance, along with its attachments, describes the SJU's video-surveillance system and the safeguards that the SJU takes to protect the personal data, privacy and other rights of those caught on the cameras (hereinafter referred to as the "Rules").

The SJU being strongly committed to the protection of personal data, privacy and other rights of its staff members and visitors, prepared these rules, which are based on the "EDPS video-surveillance guidelines[1]", (hereinafter referred to as "the guidelines") and their latest follow up[2], issued by the European Data Protection Supervisor (hereinafter referred to as the "EDPS") in the exercise of the powers conferred on him in Art. 57 of Regulation[3] 2018/1725 on the protection of personal data by Union institutions, bodies, offices and agencies (hereafter referred to as "the Regulation").

2 HOW DOES THE SJU ENSURE THAT THE VIDEO-SURVEILLANCE SYSTEM IS DESIGNED WITH PRIVACY AND DATA PROTECTION CONCERNS IN MIND AND IS COMPLIANT WITH DATA PROTECTION LAW?

2.1 Revision of the existing system

A video-surveillance system had already been operating in the SJU before the issuance of the Guidelines on 17 March 2010. Indeed, the Video-surveillance policy was adopted by Decision of the Executive Director Decision ref. SJU/ED/197 of 6 August 2012 in compliance with Video-Surveillance Guidelines by the EDPS on 17 March 2010.

From there on, the video-surveillance system has been subject to three subsequent upgrades in 2012 and 2015 and 2017 with a view to increase the security measures. **[Restricted version]**

---

[1] Available on http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf .

[2] Available on https://edps.europa.eu/data-protection/our-work/publications/guidelines/video-surveillance-follow_en

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

The present procedure is being upgraded to comply with the recommendation set forth in the guidelines (section 15).

2.2 Compliance status

The SJU processes the images in accordance with both the Guidelines and the Regulation.

2.3 Self –audit

The SJU conducted a Security Audit – Contract SJU-0142-CTR Physical Security Audit, full report included in Appendix 6 of the restricted version of these rules.

2.4 Notification of compliance status to the EDPS

The SJU performed a prior check to assess the need of a Data Protection Impact Assessment (DPIA) according to article 39 of the Regulation.

Considering that:

- The processing activity does not fall under the categories of article 39(3) of the Regulation
- Not more than two criteria from the list of Annex 1 of the Accountability on the ground guidelines[4] apply
- Annex 3 of the Accountability on the ground guidelines indicates Standard CCTV on a limited scale in the list of common processing operations not requiring a DPIA
- the limited scope of the system and that its use does not fall under the cases of section 3.3. of the guidelines requiring an impact assessment

it was not necessary to carry out a data protection impact assessment.

Following adoption of present Rules, the SJU will also notify the EDPS of its compliance status by sending them a copy thereof.

2.5 Decision-making process for the adoption of a video-surveillance policy applicable to the SJU

During this decision-making process, the SJU:

- demonstrated and documented the need for a video-surveillance system as proposed in these Rules (recommendations received from the Security Audit – Contract SJU-0142-CTR Physical Security Audit, full report included in Appendix 6 of the restricted version of these rules).
- discussed alternatives and concluded that the maintenance of the current video-surveillance system, after the adoption of the data protection safeguards proposed in these Rules, is necessary and proportionate for the purposes described in Section 1, and
- addressed the comments of the Data Protection Officer ("DPO")[5] and the Staff Committee.

[4] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies, part I: Records and threshold assessment, version 1.3, July 2019

[5] Duly appointed by SJU/ED-025 and by letter from the SJU Executive Director to the European Data Protection Supervisor dated 18th August 2009.

2.6 Transparency

The SJU Video-surveillance Rules shall be publicly made available and posted on the SJU public web and intranet with the exception to detailed aspects of this Policy which cannot be disclosed for security reasons i.e. when the preservation of confidentiality is absolutely necessary for compelling reasons. Any part which could not be disclosed for security reasons shall either be removed from the document or summarised. In such a case, this will be clearly stated in the published document.

2.7 Periodic reviews

Due to this, a periodic data protection review, every two years, will be undertaken by the Facilities & Support Services which is responsible for the safety and security of its buildings, assets, staff and visitors. The DPO will be consulted and participate in the review for compliance purposes. During the periodic reviews the SJU will re-assess that:

- there continues to be a need for the video-surveillance system,
- the system continues to serve its declared purpose, and that
- adequate alternatives remain unavailable.

3 WHAT AREAS ARE UNDER SURVEILLANCE? [Restricted version]

The video-surveillance system is located at the premises of the SJU.

Although the SJU has no camera either in the building or outside its premises in the 4th and 5th floor, it shall be noted that video-surveillance is carried out by the owner of the building in surrounding areas of the SJU premises. For clarity, the premises of the SJU cover the full surface of 5th floor, and half of the surface of 4th floor of the same building.

The SJU also does not monitor any areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others. Indeed, location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes.

4 WHAT PERSONAL INFORMATION DOES THE SJU COLLECT AND FOR WHAT PURPOSE? CONFIDENTIAL VERSION

4.1 Summary description and detailed technical specifications of the system

The video-surveillance system is a conventional static system. It records images detected by the cameras in the area under surveillance, together with time, date and identification of the camera location.

The image quality in most cases allows identification of those in the camera's area of coverage. The cameras are all fixed (there are no pan-tilt-and-zoom cameras), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around.

The SJU does not use high-tech or intelligent video-surveillance technology, does not interconnect the SJU video-surveillance system with other systems, and the SJU does not use covert surveillance, sound recording, or "talking CCTV". The technical specifications for the cameras and for the video-surveillance system as a whole (including any software and hardware) are included in Appendix 2.

4.2 Purpose of the surveillance

The SJU uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to the SJU premises and helps ensure the security of the building, the safety of the SJU staff and visitors, as well as property and information located or stored on the premises. It

complements other physical security systems such as access control systems[6] and physical intrusion control systems. It forms part of the measures to support the SJU broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the SJU, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

4.3 Purpose limitation

The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access). It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 6.4 below (in line with Section 5.7, 5.8 and 10.3 of the Guidelines).

4.4 No ad hoc surveillance foreseen

The SJU foresees no *ad hoc* surveillance operations at this time.

4.5 Webcams

The SJU has a webcam which is used for the sole purpose of meetings and web-conferences (not for video-surveillance purposes). *All users are informed and consent is sought before its use.* The images are not recorded therefore there is no retention. The system is used in relation to a meeting (such as a conference phone). It is up to the person organizing the video conference inviting attendees to explain that the meeting will use the video conferencing system. The platform is a tool, like for example a phone.

4.6 No special categories of data collected

The SJU does not collect special categories of data.

5 WHAT IS THE LAWFUL GROUND AND LEGAL BASIS OF THE VIDEO-SURVEILLANCE? CONFIDENTIAL VERSION

The use of the SJU video-surveillance system is necessary for the management and functioning of the SJU (for the security and access control purpose (described in Section 4.2 above). Therefore, in accordance with Article 5(1) (a) of the Regulation, the SJU has a lawful ground for the video-surveillance.

6 WHO HAS ACCESS TO THE INFORMATION AND TO WHOM IS IT DISCLOSED? CONFIDENTIAL VERSION

Access rights are limited to a small number of clearly identified individuals on a strictly need-to-know basis. Authorised users can access only those personal data to which their access rights refer.

Under the conditions defined in these rules (see Section 4.2 above), the following apply:

- Recorded video: only available to the following staff: Executive Director, Local Informatics Security Officer (LISO), Local Security Officer (LSO), Chief Administration Affairs, Facilities & Support Services staff members, , and the system administrator
- Live video (real-time viewing): available through a confidential and secured user profile on the SJU network and partly:

[6] Doors equipped with automated badge access.

- Partly, only available to the above listed persons and to the security guard when on-site from 17h00 onwards Monday – Thursday and 16h00 onwards on Friday.
- Partly available to the LISO, LSO, the system administrator and the accredited security guard when on-site from 17h00 onwards Monday – Thursday and 16h00 onwards on Friday.

The security guards on site have no access to the recorded video.

Detailed list of the name of the persons/ their function and their access rights is provided in Appendix 3.

6.1 Access rights

Appendix 3 clearly specifies and documents who has access to the video-surveillance footage and the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the document specifies who is authorized, under the conditions of these rules, to:

- view the footage in real-time,
- view the recorded footage,
- copy,
- download,
- delete, or
- alter any footage.

6.2 Data protection training

All SJU staff/all personnel with access rights will be given data protection training.

Data protection trainings of the outsourced security company's staff were also part of the tender specifications for the award of the security related services contracts and were taken into consideration in the evaluation report. The contractor confirmed in its technical offer that all their staff attend mandatorily a data protection training.

6.3 Confidentiality undertakings

All personnel with access rights identified in Appendix 3 above have signed a confidentiality undertaking.

6.4 Rules on transfer and disclosure

All transfers and disclosures outside the group of persons with access rights shall be documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purpose of the transfer with the initial security and access control purpose of the processing. A register of retention and transfers will be kept. The SJU DPO shall be consulted in each case. *So far there have been 3 transfers (see Appendix 5).*

No access is given to any other person and in particular to the HR sector.

In accordance with laws and regulations in force, the SJU may have to give access to local police (or to any other body entitled) to the data if needed to investigate or prosecute criminal offences.

Under exceptional circumstances, access may also be given to:

- the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF,
- those carrying out a formal internal investigation or disciplinary procedure within the SJU,
- provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining are accommodated.

6.5 Transfers and disclosures

All transfers and disclosures of CCTV footage must be formally requested in writing and documented and are subject to a rigorous assessment of the necessity for such transfer and the compatibility of the transfer with the declared security and access control purpose (see Section 10 of the EDPS Guidelines).

- Transfers to local law enforcement authorities (e.g. *Inspecteur du Police locale*) when needed, to investigate or prosecute criminal offences.

Such transfers can only be authorized following a formal written request to SJU, signed by a sufficiently highly ranked police officer or a court order, or a similar formal request, specifying the reason why the VSS images are needed as well as the location, date and time of the requested images. Each request for disclosure to local authorities is assessed by the SJU Local Security Officer (LSO) and the Facilities & Support Services Team and also the Data Protection Officer (DPO) shall be consulted.

- Image exportation and Register of transfers

Transfers may happen by exporting images from the system upon the permission of the LISO or LSO or on behalf of the Executive Director. Only the LISO or LSO, restricted team of the Facilities & Support Services in charge and the coordinator of security guards are able to export images from the system. All transfers are registered in the Log of video-surveillance recording transfers, in Appendix 5 (see Sections 7.2 and 10.5 of the EDPS Guidelines).

- Outsourced services

At the SJU, Security surveillance services, in terms of “guarding”, as well as “monitoring of alarm, intervention on premises and maintenance of security systems”, are outsourced through the following two service contracts:

SJU/LC/0375 – Lot 1 Provisions of security related services “guarding”, and

SJU/LC/0327 – Provisions of security related services “monitoring of alarm, intervention on premises and maintenance of security systems”.

Since the establishment of the SJU, the SJU has authorised three (3) transfers documented in Appendix 5

7 HOW DOES THE SJU PROTECT AND SAFEGUARD THE INFORMATION?

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organisational measures have been put in place in accordance with Section 9 of the Guidelines. These are detailed in Appendix 3.

Among others, the following measures are taken:

- the premises which host the servers storing the images recorded are secured;
- network firewalls in order to protect the logic perimeter of the IT infrastructure have been installed;
- the security of the main computer systems holding the data has been security hardened: main computer and data-monitor are stored in a secured rack, placed inside the protected data-room;
- all staff (internal and external) with access rights signed non-disclosure and confidentiality agreements;
- access rights have been granted only to the resources which are strictly necessary to allow the staff identified in Appendix 3 to carry out their jobs;

- only the system administrator, specifically appointed and by order of the controller for this purpose, is able to grant, alter or annul any access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to the criteria established Appendix 3.
- Appendix 3 contains an up-to-date list of all persons having access to the system at all times and describes their access rights in detail.
- All staff with access rights have undertaken a data protection training
- Procedure to handle data breaches foreseen in the contract

8 HOW LONG DOES THE SJU KEEP THE DATA?

The images are retained for a maximum of thirty calendar days. Thereafter, all images are deleted. If any image needs to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed.

9 HOW DO WE PROVIDE INFORMATION TO THE PUBLIC ON THE EXISTENCE OF VIDEO-SURVEILLANCE?

9.1 Multi-layer approach

We provide information to the public about the video-surveillance in an effective and comprehensive manner. To this end, we follow a multi-layer approach, which consists in a combination of the following methods:

- on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing,
- the SJU has posted these rules on the SJU intranet and public web (in its public version) for those wishing to know more about the video-surveillance practices of the SJU.

Print-outs of this Policy are available at the SJU reception desk as well as from the Facilities & Support Services which is responsible for Security aspects. An email address is provided for further enquiries (sju.security@sesarju.eu).

We also provide on-the-spot notices adjacent to the areas monitored, as listed above, are placed in the following locations:

- stairwell (4th and 5th floor) near the entrance doors equipped with automated badge access as well at the elevator entrance on the 4th and 5th floor of the building,
- near the cameras placed in both 4th and 5th corridors.

The SJU's on-the-spot data protection notice is included as Appendix 4**.**

9.2 Specific individual notice

In addition, individuals must also be given individual notice if they were identified on camera 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,
- kept beyond the regular retention period,
- transferred outside the group of persons with access rights, *or*

- if the identity of the individual is disclosed to anyone outside the group of persons with access rights.

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences. The SJU DPO shall be consulted in all such cases to ensure that the individual's rights are respected.

10 HOW CAN MEMBERS OF THE PUBLIC VERIFY, MODIFY OR DELETE THEIR INFORMATION?

Members of the public have the right to access the personal data the SJU holds on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to the Facilities & Support Services responsible for security matters at the following address: sju.security@sesarju.eu. The SJU DPO may also be contacted in case of any other questions relating to the processing of personal data.

Information on action taken on the data subject's request to exercise her/his rights shall be provided without undue delay and in any case within one month of receipt of the request. In case of complex or voluminous requests, this period may be extended by another two months, in which case the JU will inform the data subject.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the SJU to identify them from the images reviewed.

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

Possible restrictions as laid down in Article 25 of the Regulation and the upcoming SJU decision on Restrictions may apply to the above rights. For example, following a case-by-case evaluation we may have to conclude that restricting access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

11 QUERIES AND COMPLAINTS, AND RIGHT OF RECOURSE

In case of queries or complaints, please contact the

- The relevant unit at the SJU responsible for security aspects, the Facilities & Support Services at the following address sju.security@sesarju.eu, and/or
- The SJU DPO (sju.data-protection@sesarju.eu)

In addition, every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under the Regulation have been infringed as a result of the processing of their personal data by the SJU.

Before doing so, the SJU recommends that individuals first try to obtain recourse by contacting the addresses indicated in the first paragraph of the present section.

Staff members may also request a review from their appointing authority under Article 90 of the Staff Regulation.

12 ENTRY INTO FORCE

Version 2 of the present policy shall enter into force on the day following the date of its adoption. It repeals the previous Video-surveillance policy. The Executive Director may request a review of document whenever deemed necessary.

Richard Frizon
Executive Director ad interim

Brussels 9th November 2021

13 APPENDICES: [RESTRICTED VERSION]

- Appendix 4: SJU's on-the-spot data protection notice and Specific Privacy Statement for data subjects;

Appendix 4: SJU's on-the-spot data protection notice and Specific Privacy Statement for data subjects;

SESAR Joint Undertaking

for your safety and security, this zone and its immediate vicinity is under video-surveillance. Images are recorded from 17h00 to 7:00, 24 hours a day on week ends.

for further information: sju.security@sesarju.eu

Rules governing the use of video-surveillance

within the SESAR Joint Undertaking can be found on www.sesarju.eu and on the SJU's Intranet

SESAR Joint Undertaking

for your safety and security, this zone and its immediate vicinity is under video-surveillance. Images are recorded on a 24 hour / 7 basis

for more information: sju.security@sesarju.eu

Rules governing the use of video-surveillance

within the SESAR Joint Undertaking can be found on www.sesarju.eu
and on the SJU's Intranet