SPECIFIC PRIVACY NOTICE – Video-Surveillance at the SJU

Images on individuals captured by the CCTV camera system of SJU constitutes personal data, the processing of which shall comply with Regulation 2018/1725[1] (the ''Regulation'').

What is the purpose of the personal data collection?

SJU operates the video-surveillance system for controlling the access to its premises and for ensuring the safety and security of buildings, assets, staff and visitors. The Video-surveillance Policy of SJU describes the CCTV system and the safeguards that SJU takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

The use of the SJU video-surveillance system is necessary for the management and functioning of the SJU (for the security and access control purposes).

Which kind of personal information is collected?

Images of persons and objects captured in live monitoring, operating 24 hours per day, 7 days per week and stored in video-footage records of the SJU Video Surveillance system, from which individuals are recognisable in a direct or indirect manner (e.g. identification from images in combination with other information).

What is the legal basis of the processing?

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). Therefore, in accordance with Article 5(a) of the Regulation 2018/1725, the SJU has a lawful ground for the video-surveillance.

Actors in the data collection

Controller: The SESAR JU

Processors: The Corporate Support Unit. A part of the security services is outsourced to security companies that have limited access to the real-time image when it is strictly necessary for the provision of those services.

How is SJU processing the personal data?

Images of persons and objects are stored in video-footage records of the SJU Video surveillance system.

How do we protect and safeguard your information?

Password protection, secure rooms and accredited security guards.

Who has access to your information and to whom is it disclosed?

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:

- Recorded video: only available to the following staff: Corporate Support staff members, Deputy Executive Director- Corporate Affairs, and Executive Director. The outsourced security companies have no access to the recorded video.

[1] 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

- Live video (real-time viewing): available through a confidential and secured user profile on the SJU network and partly only available to the above listed persons and to the security guard when on-site, and partly to the accredited Security Guard when on-site from 17h00 onwards from Monday to Thursday, and from 16h00 onwards on Friday.

In case of security incidents or inquiries thereto, access to the CCTV footage may be transferred and disclosed to other persons. All transfers and disclosures outside the Corporate Support Unit and the security guards team are possible only after permission of the Local Security Officer, and consultation of the Data Protection Officer, and such transfers are documented in a specific register. Each transfer is subject to a rigorous assessment of the necessity of such transfer and the compatibility with the initial security and access control purpose.

Under these circumstances, access may be given to:

- Local police or if needed to investigate or prosecute criminal offences.
- The European Anti-fraud Office (OLAF) in the framework of an investigation carried out by OLAF or the investigation panel or the disciplinary board in the framework of an administrative inquiry or disciplinary proceeding, under the rules set forth in Annex IX of the Staff Regulations, provided that it can be reasonably expected that the transfers may help the investigation or prosecution of a sufficiently serious disciplinary or criminal offence.

What are your rights and how can you exercise them?

In case you want to consult the images of the SJU CCTV system on which you are captured, please contact the SJU Corporate Support Unit by email at sju.security@sesarju.eu .

Please note that on-the-spot notices with the CCTV pictogramme mark the areas within the SJU building perimeter covered by the video surveillance.

Moreover, the procedure to grant rights to data subjects includes:

- Access to the DPO's register of data processing operations;
- Requests from data subjects to the Data Controller to exercise their rights; as well as
- Detailed procedures to exercise the rights to **access, rectify, erase, block, object, notify to third parties of any rectification, erasure or blocking and not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data** intended to evaluate certain personal aspects relating to him or her, unless such decision is expressly authorised pursuant to national or Community legislation or the European Data Protection Supervisor (as required by articles 14-16 of the IDPR Regulation).

Possible restrictions as laid down in Article 25 of the IDPR Regulation can apply, based on the assessment conducted on a case by case analysis, in particular where it is necessary to safeguard the rights of the data subjects and/or the rights and freedom of others.

For how long the data is retained?

The images are retained for a maximum of **thirty calendar days**.

Complaints, concerns and recourse

Any complaint or concern shall be addressed to the data protection officer of the SJU: sju.data-protection@sesarju.eu and the Corporate Support Unit at sju.security@sesarju.eu .

Data subjects have a right to recourse to the European Data Protection Supervisor (EDPS) at any time edps@edps.europa.eu