SPECIFIC PRIVACY NOTICE – COVID-19 Pandemic – Booking system Voluntary Return to Office -

Implementation of Information Circular ref. 20-077 (COVID-19 Pandemic – Return to Office Strategy & Guidance) involves processing of personal data, which shall comply with Regulation (EU) N° 2018/1725[1] (the ''Regulation'').

What is the purpose of the personal data collection?

While teleworking remain the norm during at least Phase 1 of the SJU return to office strategy, presence at SJU premises is allowed on an exceptional basis, when so agreed with the line manager, and respecting all sanitary measures indicated by the Belgium Authorities and by the European Commission.

In this context, the purpose of the processing operations is to control the level of occupation of its premises set as "open space" and to organise the progressive and voluntary return in a way that allows the SJU staff to be closely managed in order to take reasonable precautionary measures and ensure compliance with the applicable sanitary measures to date.

Considering the exceptional circumstances, this privacy notice will be updated as the return to office strategy implementation evolves.

Which kind of personal information is collected?

The following categories of personal data are processed:

- Personal details (name and position);
- Date(s) and period(s) of time (am/pm) of presence at SJU premises.

What is the legal basis of the processing?

The legal basis of the processing is:

- Art. 5.1 (b) of R(EU) 2018/1725: Information Circular ref. 20-077 (COVID-19 Pandemic – Return to Office Strategy & Guidance);
- Art. 5.1 (d) of R(EU) 2018/1725 where the data subject has given explicit consent to the publication of his/her personal details on the staff presence list.

Actors in the data collection

- **Controller:** The SESAR JU.
- **Internal Processor:** Facility team, ICT team, LISO and LSO.

How is SJU processing the personal data?

The collection of personal data and establishment of the list is made electronically (i.e. by e-mail) by the Facility team.

Every week, the persons willing to come to the SJU premises shall send to the Facility and ICT mailboxes a request to be present at the SJU premises for a given period of time and clarify if he/she consents to

[1] Regulation (EU) N° 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 ("EUDPR").

the publication of his/her name, date, and period of presence on I-DMS (see below) according to the template provided by the Facility team.

The staff allowed to return to the office shall receive an e-mail of confirmation of the booking of a space at the SJU premises at the requested period of time if his/her request complies with all the measures and restrictions contained in IC 20/077 and any other EC guidance applicable to the situation.

As a result of this process, every Friday after 15:00 and until general de-confinement (Phase 4 under IC 20/077), the Facility team will compile the received data of the persons that have required to be at the SJU premises on the following week and whose requests are compatible with all measures mentioned in IC ref. 20-077 in the following documents:

1. A "***safety and security register***": this database will contain all names, functions and time period of presence of staff at the SJU premises with restricted access by the Facility team, ICT team, LISO and LSO.
2. A "***weekly contact table***": this database - accessible to all SJU employees, PMU staff, ICT Coordination, ICT Support, Reception and D&D SDSS Team (hereafter referred to as "***intramuros staff***") on IDMS - will identify people exceptionally present at the office on a weekly basis.

How do we protect and safeguard your information?

- Organisational measures: workflows, access rights and access control.
- Technical measures: use of secured equipment and IT tools, e.g. locked cupboards, secure connections, firewalls, etc.

In particular:

- ***The safety and security register*** will be stored on IDMS with restricted access given to the Facility team, ICT team, LISO and LSO. The personal information contained in this register list will be stored by the Facility team on their dedicated IDMS folder;
- ***The weekly contact table*** based on explicit consent for "intramuros" publication will be not be modifiable (i.e. in "read only" mode), stored on IDMS and be only accessible to the intramuros staff for one week.

Access to IDMS is electronically secured with access rights granted on a case-by-case basis.

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

The safety and security register:

- Facility team, ICT team, LISO and LSO.

The weekly contact table:

- SJU all employees, PMU staff, ICT Coordination, ICT Support, Reception and D&D SDSS Team ("intramuros staff").

What are your rights and how can you exercise them?

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 automated decision making.** The content of these rights is detailed in the Data Protection Notice page in SJU website, which contain also information about the contact points and recourse (including EDPS http://www.edps.europa.eu and edps@edps.europa.eu, and SJU DPO sju.data-protection@sesarju.eu) as well as detailed information on the exercise of the rights and information on possible restrictions.

Possible restrictions as laid down in Article 25 of the Regulation and the upcoming SJU decision on restrictions may apply.

For how long the data is retained?

- ***The safety and security register*** will be stored by the Facility team on their dedicated IDMS folder for one year with restricted access for the sole purpose of being used in safety, security, or sanitary dossiers if needed;
- ***The weekly contact table*** will be deleted upon expiration of the week of presence, the following Friday evening and substituted by an updated table for the following week.

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 Facility team at facility@sesarju.eu.
- The ICT team at ict-support@sesarju.eu.

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