



SHIFT2RAIL JOINT UNDERTAKING VIDEO-SURVEILLANCE POLICY

Adopted by ED Decision 20-16
Version 1.0p

Version 1.0p (public version)

Drafted and reviewed by	Isaac GONZÁLEZ GARCÍA – Chief Legal & Data Protection Officer Fabien GENTNER – IT & Security Officer Vincent Declerfayt – Head of Administration and Finance
Approved by	Carlo Borghini – Executive Director
Date of approbation	Ares workflow
Maintenance	Fabien GENTNER – IT Officer

DOCUMENT HISTORY

Version	Date	Comment
1.0	20/10/2020	Document review
1.0p	16/11/2020	Public version

Table of Contents

1. Purpose and scope of the S2R JU Video-surveillance Policy.....	4
2. How do we ensure that our video-surveillance system is designed with privacy and data protection concerns in mind and is compliant with data protection law?.....	4
2.1 Compliance status	4
2.2 Self-audit.....	4
2.3 Notification of compliance status to the EDPS.....	4
2.4 Contacts with the relevant data protection authority in the Member State.....	4
2.5 Director's decision and consultation	5
2.6 Transparency	5
2.7 Periodic reviews.....	5
2.8 Privacy-friendly technological solutions.....	5
3. What areas are under surveillance?	6
4. What personal information do we collect and for what purpose?	6
4.1 Purpose of the surveillance	6
4.2 Purpose limitation	6
4.3 No ad hoc surveillance foreseen	6
4.4 Webcams	6
4.5 No special categories of data collected.....	7
5. What is the lawful ground and legal basis of the video-surveillance?.....	7
6. Who has access to the information and to whom is it disclosed?.....	7
6.1 In-house security staff and outsourced service provider.....	7
6.2 Access rights	7
6.3 Data protection training	7
6.4 Transfers and disclosures.	7
7. How do we protect and safeguard the information?	8
8. How long do we keep the data?	8
9. How do we provide information to the public?.....	9
9.1 Multi-layer approach	9
9.2 Specific individual notice	9
10. How can members of the public verify, modify or delete their information?.....	9
11. Right of recourse	10

1. Purpose and scope of the S2R JU Video-surveillance Policy

For the safety and security of its buildings, assets, staff and visitors, our JU operates a video-surveillance system. This Video-surveillance Policy, along with its annexes, describes the JU's video-surveillance system and the safeguards that the S2R JU takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

2. How do we ensure that our video-surveillance system is designed with privacy and data protection concerns in mind and is compliant with data protection law?

2.1 Compliance status

The S2R JU processes the images in accordance with both the Video-Surveillance Guidelines¹ issued by the European Data Protection Supervisor ("Guidelines") and Regulation (EU) 2018/1725 on the protection of personal data by the Community institutions and bodies.

2.2 Self-audit

The system was subject to a camera by camera site audit. With the objective to minimise the monitoring of areas that are not relevant for the intended purposes, two installation options were proposed by the security company and one of these has been approved for adoption. Camera locations and viewing angles were chosen accordingly. Since previously no video-surveillance policy existed, the result of the audit is this policy.

2.3 Notification of compliance status to the EDPS

Considering the limited scope of the system, it was not necessary to carry out a formal impact assessment or to submit a prior checking notification to the EDPS.

Simultaneously with adopting this Video-surveillance Policy, we also notified the EDPS of our compliance status by sending them a copy of our Video-surveillance Policy. The EDPS provided several recommendations which were duly taken into consideration and implemented.

2.4 Contacts with the relevant data protection authority in the Member State

Due to the fact that the cameras are not recording outside the building, there is no need to contact the local data protection authority.

¹ https://edps.europa.eu/sites/edp/files/publication/10-03-17_video_surveillance_guidelines_en.pdf

2.5 Director's decision and consultation

The decision to use the current video surveillance system and to adopt the safeguards as described in this Video-surveillance Policy was made by the Director of the S2R JU after consulting:

- The JU's IT and Security Officer,
- The JU's Data Protection Officer,
- The Head of Administration and Finance.
- The Staff Committee

During this decision-making process, the S2R JU:

- demonstrated the need for a video-surveillance system
- discussed alternatives and concluded that the current video-surveillance system, after the adoption of the data protection safeguards proposed in this policy, is necessary and proportionate for the purposes described in Section 1, and
- addressed the concerns of the DPO and the Staff Committee: The proposed policy has been presented to the Staff committee who was invited to outer its opinion and potential comments have been and will be taken into account for further development of this policy.

2.6 Transparency

The Video-surveillance Policy can be consulted on demand by way of the access to documents procedure. In this case, information is only omitted, when the preservation of confidentiality is necessary for compelling reasons (e.g. for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals). For further information on transparency and access rights, please also refer to section 10 of this policy.

2.7 Periodic reviews

The IT and Security Officer together with the DPO undertake to a periodic data protection review every two years. During the periodic reviews, we 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.

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether our Video-Surveillance Policy continues to comply with the Regulation and the Guidelines (adequacy audit), and whether it is followed in practice (compliance audit).

2.8 Privacy-friendly technological solutions

When commissioning new equipment for the system and whenever possible, the S2R JU will use the best available privacy-friendly technological and procedural solutions.

3. What areas are under surveillance?

The S2R JU CCTV system monitors the minimum area necessary to ensure the safety and security of the premises, in particular sensitive areas and restricted access areas. They do not monitor any area under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others. The 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 do we collect and for what purpose?

4.1 Purpose of the surveillance

The S2R JU uses its video-surveillance system to protect its premises and assets for safety, security and access control purposes only. In addition, the video-recordings can be used to investigate any physical security incident that occurs as well as a formal disciplinary or criminal investigation (see section 6.4). The video-surveillance system helps monitor access to our offices, as well as safeguards property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support our broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secured 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 S2R JU, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

4.2 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 case of transfers of data to third parties, the S2R DPO will be first consulted and the transfers will be included in the register of data transfers. The recording and deletion are automatic. Any other action (manual copy/deletion) will also be included in the register.

4.3 No ad hoc surveillance foreseen

We foresee no ad hoc surveillance operations for which we would need to plan at this time.

4.4 Webcams

The S2R JU does not use webcams for security or surveillance purposes.

4.5 No special categories of data collected

The S2R JU Video surveillance system does not aim at collecting special categories of data such as racial or ethnic origin, religious beliefs or data related to health or sexual orientation.

The S2R JU CCTV system monitors the minimum area necessary to ensure the safety and security of the premises as described in point 3.

5. What is the lawful ground and legal basis of the video-surveillance?

The use of our video-surveillance system is necessary for the management and functioning of the S2R JU (for the security and access control purpose described in Section 4.2 above). Therefore, we have a lawful ground for the video-surveillance, as required under Regulation (EU) 2018/1725 and is based in a public Interest (Article 5(1) a) of Regulation 2018/1725). This policy, in turn, forms part of the broader security policies adopted by our JU.

6. Who has access to the information and to whom is it disclosed?

6.1 In-house security staff and outsourced service provider

Recorded videos are accessible to the IT and Security Officer only. Under exceptional circumstances and upon request, physical access to the video-surveillance system and the recordings can be granted and made accessible to the external service provider in charge of the maintenance.

6.2 Access rights

Access to the video-surveillance footage and/or the technical architecture of the video-surveillance system is only granted to the S2R JU IT and Security Officer, only for security purposes in the case that an incident is recorded during the system's operating hours. Further access rights are only granted in very specific cases (see section 6.4) and only if explicitly requested.

6.3 Data protection training

Training is provided for each new member of the staff and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights.

6.4 Transfers and disclosures.

The S2R JU does not undertake any regular or routine transfers. In very specific cases, data may be disclosed to the security services of other European Institutions or to security, judicial, or law enforcement authorities of EU member states, only for the purpose of ongoing inquiries or to investigate or prosecute criminal offences. Such transfers shall only be carried out on explicit request and be recorded. In case of a national police, a court or

other national Belgium authorities request the disclosure of recordings, the S2R JU will introduced a formal written request be made according to the requirements of the Belgium national law regarding form and content. The S2R JU will only disclose the recordings if the European Commission would also have been required or at least permitted to make the disclosure under similar circumstances. The request should specify, as closely as possible, the reason why the video-surveillance footage is needed as well as the location, date and time of the requested footage. The S2R JU may, in most cases, accommodate requests from national police when the recordings are necessary to investigate or prosecute criminal offences provided that data are requested in the framework of a specific criminal investigation. However, no general requests should be accommodated for data mining purposes.

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,
- the Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Institution, 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.

7. How do we 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. Among others, the following measures are taken:

- Secure premises, protected by physical security measures, host the servers storing the images recorded;
- The system operated on a separate, disconnected and private network with no external remote access, which excludes any possibility of intrusion and IT security breach;
- Network firewalls protect the logic perimeter of the IT infrastructure;
- The main computer systems holding the data are security hardened;
- All staff (external and internal) signed non-disclosure and confidentiality agreements;
- Access rights are granted on a need-to-know basis;
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons.

8. How long do we keep the data?

We should be able to provide the recordings upon request, following an incident and before their automated deletion. Our CCTV system is not linked to the building security system nor a managed system and only accessible upon request by strictly limited staff: the S2R JU IT and Security Officer and our supplier as backup if required. Given the lack of

remote access and potential lack of internal staff to access the recordings, we can only rely on the delay from our supplier to come onsite and check the requested recordings.

A retention period of 14 calendar days is applied, the necessary period to ensure that the images could be retrieved before automated deletion. The purpose of this retention period is to guarantee that the S2R JU has time to further investigate a security incident or use it as an evidence, in particular in case of disciplinary or criminal investigation (see section 6.4). Therefore, taking into consideration the size of the JU, the human resources dealing with CCTV, the practices currently in place in other EU Bodies and the cost-estimate, the 14 days are considered acceptable. Their retention is rigorously documented and the need for retention is periodically reviewed. In case this retention period shall be extended (e.g.: images may be kept longer to facilitate the work of investigatory bodies in the framework of a formal disciplinary or criminal investigation) the records will be included in the register of recordings retained beyond the retention period.

9. How do we provide information to the public?

9.1 Multi-layer approach

We provide information to the public about the video-surveillance in an effective and comprehensive manner. To this end, on-the-spot notices are posted at the entrance of the S2R JU premises to alert the public to the fact that the premises are equipped with a monitoring system.

9.2 Specific individual notice

In addition, individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) 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,
- the video recording is kept beyond the regular retention period,
- the video recording is transferred outside the security unit, *or*
- the identity of the individual is disclosed to anyone outside the security unit.

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences². The JU's DPO is 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 we hold 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:

² Other exceptions under Article 20 of the Regulation may also apply in exceptional circumstances

Shift2Rail Joint Undertaking

Data Protection Officer

White Atrium building, 2nd Floor

Avenue de la Toison d'Or 56-60

B1060

Brussels/Belgium

E-mail address: Data-Protection@s2r.europa.eu

The JU's DPO may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the IT and Security Officer responds to any enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex cases, access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest. The unit must do its best to respond earlier, especially if the applicant establishes the urgency of the request.

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 security staff 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.

An access request may be refused when an exemption under Article 25(1) of Regulation 2018/1725 applies in a specific case. 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. For more information see the internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the S2R JU published at <https://shift2rail.org/about-shift2rail/reference-documents/functioning-of-the-ju/>

11. Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 2018/1725 have

been infringed as a result of the processing of their personal data by the JU. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

- the IT and Security Officer of the S2R JU
- the data protection officer of the S2R JU

DPO/ Chief Legal Officer
White Atrium building, 2nd Floor
Avenue de la Toison d'Or 56-60
B1060
Brussels/Belgium
E-mail address: Data-Protection@s2r.europa.eu

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

Detailed information on how S2R JU processes personal data is included in the S2R JU Data Protection & Legal Notices (<https://shift2rail.org/terms-of-use/>) and the specific data privacy policy (<https://shift2rail.org/about-shift2rail/reference-documents/functioning-of-the-ju/>).

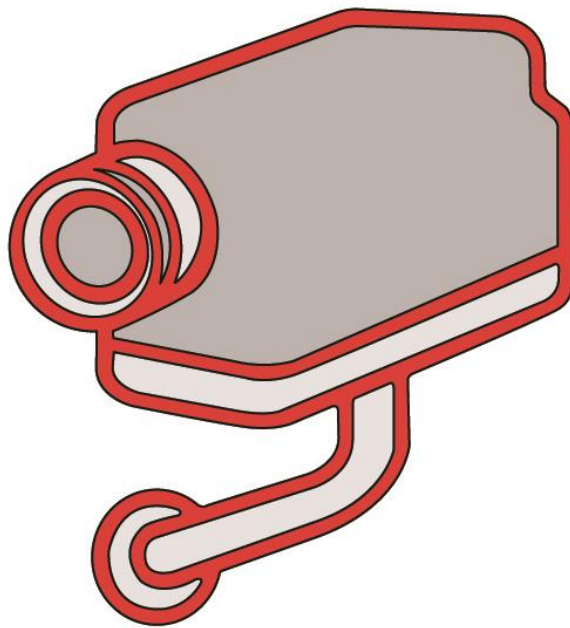
For reasons of transparency, this processing operation is included in the S2R JU record of processing activities (<https://shift2rail.org/dprester/>).

* * *

Annexes to the Video-surveillance Policy:

- Annex 1 – **S2R JU's on-the-spot data protection notice**

**ANNEX 1:
The S2R JU's on-the-spot data protection notice**



Surveillance par caméra - Loi du 21 mars 2007
Camerabewaking - Wet van 21 maart 2007

Shift2Rail Joint Undertaking
Avenue de la toison d'or, 56-60
1060 Brussels

Data-protection@s2r.europa.eu

<https://shift2rail.org/dpreregister>