GSA video-surveillance Policy

Adopted by the Director's Decision on 29 August 2017

(ref. GSA-SEC-CSO-POL-233177)

1. Purpose and scope of the Policy

For the safety and security of its buildings, assets, staff and visitors, as well as the European Union classified information, the European GNSS Agency (hereinafter "the GSA" or "the Agency") operates a video-surveillance system. This GSA video-surveillance Policy, along with its attachments, describes the Agency's video-surveillance system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on cameras.

2. The GSA video-surveillance system (CCTV system)

2.1 Compliance status

The Agency processes the images in accordance with both the Guidelines and Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies.

Due to the high volume of EU classified information handled at the GSA and the sensitive nature of the tasks carried out and of the information managed, images recorded from CCTV system are kept for a period of one month from the day they were recorded. This deviation from the Guidelines has been duly reported to the European Data Protection Supervisor (hereinafter "the EDPS").

2.2 Notification of compliance status to the EDPS

In spite of the limited scope of the CCTV system, a formal impact assessment has been carried out, following EDPS recommendation (see the Attachment).

2.3 Contacts with the relevant data protection authority in the Czech Republic

The competent data protection authority in the Czech Republic (*Úřad na ochranu osobních údajů, UOOU or The Office for Personal Data Protection*) was informed both by the hosting entity, the Czech Ministry of Finance (which is the owner of the GSA HQ building and the CCTV system) and the GSA; its concerns and recommendations were taken into account. In particular, the on-the-spot notice is also available in Czech.

2.4 Director's decision and consultation

The decision to use the current CCTV system and to adopt the safeguards as described in this Policy was made by the Executive Director of the Agency after consulting the head of the GSA Security Department and the GSA Data Protection Officer.

During this decision-making process, the Agency

- demonstrated the need for a video-surveillance system as proposed in this policy,

- concluded that the maintenance of the current CCTV system, after the adoption of the data protection safeguards proposed in this policy, is necessary and proportionate for the purposes described in Section 1,
- addressed the concerns of the GSA DPO and EDPS.

2.5 Transparency

The Video-Surveillance Policy has two versions, a version for restricted use and a public version available and posted on the GSA internet and intranet sites. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons, especially for security reasons or to preserve the confidentiality of sensitive information or to protect the privacy of individuals.

2.6 Periodic reviews

A periodic data protection review will be undertaken by the GSA Security Department every three years. During the periodic reviews, especially the following topics will be re-assessed:

- the continuation of the need for the video-surveillance system,
- that the system continues to serve its declared purpose,
- that adequate alternatives remain unavailable,
- potential need to change the system or this Policy due to changed legal requirements, the Regulation and EDPS Guidelines,
- issues addressed in previous reports.

3. Areas under surveillance

The CCTV cameras are located at entry and exit points of the GSA HQ building, in the lobby/reception area, staircases, corridors, roofs and external ledges, as well as nearest pavements around the building (especially the areas under the GSA higher floors extensions).

There are no other cameras elsewhere either in the building or outside of it. No monitoring takes place of areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and similar. 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.

Monitoring outside the GSA HQ building of the territory of the Czech Republic is limited to an absolute minimum, in order to safeguard the external security perimeter of premises only. The cameras are not to focus on private homes, gardens and other areas of private property; the external provider's security staff monitoring the cameras has been instructed accordingly. All the external provider's security staff also signs a confidentiality agreement.

4. Collected personal information

4.1 Summary description of the system

The CCTV system is a conventional static system of the GSA Headquarters building, located at Janovskeho 438/2, Prague 7, Czech Republic. It records digital images 24 hours a day, 7 days a week. The image quality can allow identification of those in the camera's area of coverage (subject to light

conditions and distance). The cameras are all fixed, with only limited number of cameras being pan-tilt-zoom cameras. Unless an immediate response to an event is required, the Security Centre staff must not direct cameras at an individual or private property, without a justified authorisation by the Central Security Office.

No high-tech or intelligent video-surveillance technology is used, neither any interconnection of the video-surveillance system to other systems, nor covert surveillance nor sound recording. No webcams are used, either.

4.2 Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purposes of security and access control. The CCTV system helps to ensure the security of the building, safety of the staff and visitors, as well as property and information located or stored on the premises, including the EU classified information. It complements other physical security systems such as access control system (ACS) and physical intrusion control systems. It helps prevent, deter and, if necessary, to investigate unauthorised physical access, including access to Secured Areas or IT infrastructure. In addition, video-surveillance helps prevent, detect or investigate theft of equipment or assets owned by the Agency, visitors of staff, and threats to the safety of visitors or personnel (e.g. fire, physical assault).

4.3 Purpose limitation

The system is not used for any other purpose (e.g. it is not used to monitor the work of staff or to monitor attendance). Neither is the system used as an investigative tool (other than investigation physical security incidents such as thefts or unauthorised access); only in exceptional circumstances the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 5.2 below.

5. Access to the information

5.1 In-house security

Images taken by the cameras are observed in real time by the external provider's security staff in the Security Centre, with limited access. Recorded video images are accessible only on specifically dedicated computers by the staff of the Central Security Office (CSO) and empowered Security Centre operators. The access is password-protected.

5.2 Security Centre

The Security Centre is manned only by the staff employed by the security service provider.

The Security Centre Operator will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

Access to the Security Centre is strictly limited. Visitors must first obtain permission from the LSO or CSO manager and must be accompanied by a CSO staff throughout the visit. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

Security Centre Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists, access will be refused.

If out of hours emergency maintenance arises, the Security Centre Operators must be satisfied of the identity and purpose of contractors before allowing entry.

A logbook is maintained in the Security Centre. Full details of visitors including time/data of entry and exit will be recorded.

5.3 Transfers and disclosures

All transfers and disclosures outside the Security Department are documented and subject to an assessment of the necessity of such transfer. The register of retention and transfers shall be kept by the GSA Central Security Office. If the transfer regards a GSA staff member, the GSA DPO is consulted.

No access is given to management or human resources.

Local police or judicial authorities may be given access if needed to images of the GSA HQ surroundings, in order to investigate or prosecute criminal offences. In such a case, a justified request must be sent to and approved by the Central Security Office.

A record will be maintained of the release of media to the Police or other authorised applicants. A register will be available for this purpose.

Viewing of Data by the Police must be recorded in writing and in the logbook and need prior written approval of the CSO.

The GSA also retains the right to refuse permission for the Police to pass to any other person the Media or any part of the information contained thereon. On occasions when a Court requires the release of an original Media this will be produced from the secure evidence Media store, complete in a sealed bag.

The Police may require the GSA to retain the stored data for possible use as evidence in the future. Such Media will be properly indexed and properly and securely stored until they are needed by the Police (see Section 7).

Under exceptional circumstances, access may also be given to:

- the European Anti-fraud Office (OLAF) in the framework of 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 the Staff Regulations of the Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Agency,

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.

6. Protection of information

In order to protect the security of the CCTV system, including personal data, a number of technical and organisational measures have been put in place, in particular:

- secure premises, protected by physical security measures, host the servers storing the recorded images,
- obligatory personal security clearance for all the staff, including outsourced personnel, who has the access to the system and/or the images recorded,
- access rights to the CCTV system are granted only to those resources which are strictly necessary to carry out their jobs.

7. Data retention

The images are retained for one month. 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. In such cases following procedures must be strictly adhered to:

- Each media must be identified by a unique mark.
- Before using each media must be cleaned of any previous recording (if the media is rewritable,
- LSO shall register the date and time of media insert, including media reference;
- Media required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence media store. If a media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by LSO, dated and returned to the evidence data store.

8. Breach of the Policy

Any breach of this GSA Video-surveillance policy, including breaches of security, will be investigated by the Local Security Officer (LSO).

9. Informing the public

The public is informed about the video-surveillance in an effective and comprehensive manner. To this end, a multi-layer approach is followed, consisting of 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, and
- posting a note on the GSA video-surveillance policy on the GSA internet site. This note is also available at the GSA HQ reception desk.

This Policy is also published on the GSA Intranet.

10. Access, verification, modification or deleting the information

Members of the public have the right to access the personal data held 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 Head of the Security Department (cctv@gsa.europa.eu). He/she may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the Security Department responds to an 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. In any case, the access must be granted or a final reasoned answer must be provided within three months at the latest.

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 and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case – e.g. when restricting the access may be necessary to safeguard an investigation of a criminal offence, or in order to protect the rights and freedoms of others.

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 45/2001 have been infringed as a result of the processing of their personal data by the Agency.

Before doing so, it is recommended that individuals first try to obtain recourse by contacting:

- the Head of the GSA Security Department (see above), and/or
- the GSA Data Protection Officer (dpo@gsa.europa.eu)

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