EMSA Video-Surveillance Rules

SECURITY RULES

Version: 1.1
Date: 01/08/2021

EMSA

Document History

Version	Date	Changes	Prepared	Approved
1.0	02/05/2016	None	A.2	ED
1.1	01/08/2021	CCTV Rules adapted to the changes in EMSA's organisation and chapter 3 updated to reflect a technical upgrade of the CCTV system in the Agency.	4.2	ED

Table of Contents

1. Purpose, scope and legal basis of the Agency's Video-Surveillance Rules

1.1 Purpose and scope

For the safety and security of its buildings, assets, staff and visitors, the European Maritime Safety Agency (the Agency) operates a video-surveillance system. These Video-Surveillance Rules, along with their attachments, describe 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 individuals whose images may be caught by the cameras.

The purpose of the video surveillance system is the reduction and prevention of security incidents. The system helps to ensure the security of the buildings, the safety of staff and visitors, as well as property and information located or stored on the premises, by means of controlling access to the Agency buildings in compliance with Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and the applicable Portuguese legislation as well as the European Data Protection Supervisor (EDPS) Guidelines.

The video surveillance system, which operates through a CCTV camera system, complements other physical security measures, such as access control systems and physical intrusion control systems. It forms part of all the security measures taken within the Agency and helps to prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, ICT infrastructure, or operational information. In addition, video surveillance helps to prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, or threats to the safety of personnel working at the offices (e.g. fire, physical assault).

1.2 Legal basis

These Rules are based and framed by the following laws and regulations:

- Regulation (EC) No 45/2001of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (the Regulation 45/2001);
- The European Data Protection Supervisor Video-Surveillance Guidelines (Guidelines) on 17 March 2010 and Video-Surveillance - Follow-up from 2013;
- Lei n.º 67/98 de 26 de Outubro, Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados);
- Lei nº 35/2004 de 29 de Julho (Regulamento Do Código Do Trabalho);
- Lei nº 49/2008 de 27 de Agosto (Lei de Organização da Investigação Criminal);
- Lei nº 34/2013 de 16 de Maio (Regime Do Exercício Da Atividade De Segurança Privada.

2. Specific characteristics of the Agency video-surveillance system

2.1 Revision of the existing system

A video-surveillance system had already been operating in the Agency before the issuance of the Video-Surveillance Guidelines by the European Data Protection Supervisor ("Guidelines") on 17 March 2010: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf and the “Video-Surveillance - Follow-up” from 2013: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-02-13_Report_CCTV_EN.pdf

The Agency procedures, however, are hereby being revised to comply with the recommendations set forth in the above Guidelines.

2.2 Compliance status

The Agency processes the images in accordance with both the Regulation (EC) No 2018/1725 and the respective EDPS Guidelines on the protection of personal data by the EU institutions and bodies.

Considering the results of a threshold assessment (attached), it was concluded that a DPIA on the assessment of the risks posed by the standard operation of the system was necessary. Such DPIA was carried out in accordance with the applicable provisions of Regulation 2018/1725 and the relevant Guidelines and templates.

The Executive Director, Staff committee and the Agency's DPO have been consulted by means of a Note, enclosed into the ARES Workflow requiring either a 'visa' or a signature of the file.

2.3 Self-audit

The system is subject to a self-audit on an ad-hoc basis.

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

The competent data protection authority in Portugal (Comissão Nacional de Protecção de Dados) was informed about the installation of the video-surveillance system on the outside of the building. On the-spot notices on video-surveillance are also available in Portuguese language.

2.5 Director's decision and consultation

The decision to use the current video-surveillance system and to adopt the safeguards as described in these Video-Surveillance Rules was made by the Director of the Agency after consulting the Agency's Security Officer (Head of Unit 4.2), the Agency's Data Protection Officer and the Staff Committee.

During this decision-making process, the Agency demonstrated and documented the need for a video-surveillance system as proposed in 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 concerns of the DPO and the Staff Committee.

2.6 Transparency

The Video-Surveillance Rules have two versions, a version for restricted use and this public version available and posted on Agency internet: http://emsa.europa.eu/ and intranet sites at http://emsanet/. This public version of the Video-Surveillance Rules contains a summary information with respect to particular topics or attachments. Information is only omitted from the public version when the preservation of confidentiality is absolutely 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).

2.7 Periodic reviews

A periodic data protection review will be undertaken by the Unit 4.2 every two years save in justified cases may be carried on more frequently. During the periodic reviews the following aspects of the system will be re-assessed:

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

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether the Video-Surveillance Rules continue to comply with the Regulation and the Guidelines (adequacy audit), and whether they

are followed in practice (compliance audit). Copy of the periodic report will also be attached to these Video-Surveillance Rules in Attachment 1.

3. Areas under surveillance

The video-surveillance system consists of 91 fixed cameras. A map with the location of the cameras is included as Attachment 2.

Based on their type and location the cameras are divided into three categories:

1. Six (6) external cameras of the 'dome' type are located on the west and south facades of the Agency building. They are movable (head) type of cameras with a 'zoom' function;

2. Twelve (12) external cameras of the 'bullet' type and 'fixed dome bullet' type are located on the east and north facades of the Agency building, internal garden, courtyard and the rooftops.

3. Nineteen (19) cameras are located as fixed cameras inside of the Agency building. They are facing the most important points of the building from a security perspective, i.e., main hall, entrance doors, evacuation exits, Data Centre doors (ICT server room, including servers for sensitive information) and other crucial points of the building.

The above three categories of cameras are operational on a 24/7 basis ('Recording Mode' - on / 'View Mode' - on) – the 'live image' is displayed permanently on the CCTV monitors and the footage is recorded on the server.

Monitoring outside EMSA building on the territory of Praça Europa in Lisbon is limited to an absolute minimum, meaning that the CCTV cameras are located and installed in a way to face only the entrance points of the Agency's building and the most exposed and particularly vulnerable points of the building from a security perspective (i.e. glazed walls on the ground floor), as indicated in the description above.

For the cameras on the outside of the building, the necessity of such operation is rooted in the fact that EMSA's Headquarters is located in the heart of the city with a lot of traffic around it, including a thriving nightlife. As such, this location elevates the level of security risk for the Agency's premisses and operations.

4. Fifty-four (54) cameras are located inside of the Agency building and cover the common areas such as corridors and hallways. They operate on a daily basis between 20:00h and 8:00h and weekends (out of working hours) in 'Recording Mode' - on / 'View Mode' – off. It means that 'live image' is not displayed on the CCTV monitors and is not available for security guards. In case of reported incident, the access to the recorded footage can be available on the server for authorised persons only, for period of 30 days.

Operation of the internal cameras on 24/7 modus is necessary because of the 24/7 operation of certain services at the Agency, which present the highest security vulnerability, for example the MSS Centre.

Besides the cameras mentioned above, there are no cameras elsewhere either in the building or outside of it. There is no monitoring of areas 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. Type and purpose of the surveillance

4.1 Summary description and detailed technical specifications for the system

The Agency video-surveillance system (as described in chapter 3 above) is a conventional system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date, and location. All cameras operate daily, as described under point 3 'Areas under surveillance' above. The image quality normally allows identifications of persons recorded within the

camera's area of coverage. The cameras are all fixed in a way that they cannot be used by the operators to follow individuals around.

The Agency does not use high-tech or intelligent video-surveillance technology, does not interconnect its system with other systems nor engages in covert surveillance, using 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 Attachment 3.

4.2 Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to the Agency building and helps ensure the security of the building, the safety of the 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 and physical intrusion control systems. It forms part of the measures to support Agency's 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 Agency, 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 for purposes 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.

4.4 Ad hoc surveillance foreseen

At present the Agency does not foresee *ad hoc* surveillance operations which would need special planning.

4.5 Webcams

There are no webcams located in the Agency premises, that are used for the surveillance purpose. All webcams which are integral elements of personal computers or A-V conference systems can be used for communication purposes only.

4.6 Special categories of data collected

The Agency does not collect special categories of data while operating the CCTV System.

5. Legal basis of the video-surveillance

The use of our video-surveillance system is necessary for the management and functioning of the Agency (for the security and access control purpose described in Section 4.2 above). Therefore, the Agency has a lawful ground for the video-surveillance . A more detailed and specific legal basis for the video-surveillance is provided in these Video-Surveillance Rules (paragraph 1.2 above). These Rules form part of the Security Rules adopted by the Agency.

6. Access and disclosure of information

6.1 In-house security staff and outsourced security-guards

Recorded video footage is accessible to the in-house security staff only. Live video footage is also accessible to security guards on duty. These security guards work for a licensed security company, contracted by the Agency. A copy of the contract with this security company is included in Attachment 4.

6.2 Access rights

These Rules for Video-Surveillance specify who has access to the video-surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the right to:

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

6.3 Data protection training

All personnel with access rights, including the security guards, are given 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 Confidentiality undertakings

After the training each staff member with access rights also signs a confidentiality undertaking. This undertaking was also signed by the contracted security company. Templates of these confidentiality undertakings are attached as Attachment 5.

6.5 Transfers and disclosures of information

All transfers and disclosures of information outside the responsible personnel are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing. The register of retention and transfers is included in Attachment 6. The DPO of the Agency is consulted in each case thereof. No access is given to management or human resources.

Local police may be given access if needed to investigate or prosecute criminal offences. The the Agency Security Officer shall be responsible to give authorisation to provide information and/or images to the local police. Every occasion of a request and provided authorisation shall be documented based on the template Disclosure Request Form, Attachment 8 to these Rules.

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 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.

7. Protection and safeguarding of 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; network firewalls protect the logic perimeter of the IT infrastructure and the main computer systems holding the data are security hardened.
- Administrative measures include the obligation of all contractors' personnel having access to the system (including those maintaining the equipment and the systems) to have relevant security documentation under national law.
- All staff (external and internal) with access rights signs confidentiality undertakings.
- Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
- 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. Any provision, alteration or annulment of access rights is made pursuant to the criteria established in the Agency rules and mechanisms in place.

8. Storing of the data

The procedure for retention of images is in accordance with Regulation 2018/1725. The retention time complies with the applicable Portuguese legislation which requires data storage of 30 days, after which images are deleted automatically.

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. A copy of the register of retention and transfers is included in Attachment 6.

The system is also monitored live by the security guard in the downstairs building reception 24 hours a day.

9. Provision of information to the public

9.1 Multi-layer approach

The Agency provides information to the public about the video-surveillance in an effective and comprehensive manner. It presents a multi-layer approach, which consists 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;
- These Video-Surveillance Rules are made available on Agency's intranet and also on its internet sites. For purposed of confidentiality and protection of the legitimate interests, certain attachments are not publicly disclosed;
- Print-outs of these Video-Surveillance Rules are also available from Agency's Security Officer upon request;
- A phone number and an email address are provided for further enquiries (general the Agency contact points).

The Agency also provides on-the-spot notice adjacent to the areas monitored. Notices are placed near the main entrance, the elevator entrances and in the parking garage within the Agency parking area and at the entry to the parking garage.

The Agency's on-the-spot data protection notice is included as Attachment 7.

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,
- kept beyond the regular retention period,
- transferred outside the 4.2 Unit, or
- if the identity of the individual is disclosed to anyone else but the Security Officer.

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 Agency DPO is consulted in all such cases to ensure that the individual's rights are respected

10. Verification, modification or deletion of information

Members of the public have the right to access their personal data the Agency 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 Agency Security Officer. The Security Officer may also be contacted in case of any other questions relating to the processing of personal data via the video surveillance system.

Whenever possible, the Security Officer 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. Even in the most complex of cases access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest. The Unit 4.2 shall make its best efforts 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 shall also provide a recent photograph of themselves that allows the security staff to identify them from the images reviewed.

At this time, the Agency does not charge applicants for requesting a viewing or a copy of their recorded images. However, the Agency reserves 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 of Regulation 2018/1725 applies in a specific case as described by 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 European Maritime Safety Agency (EMSA), available as a publication at the OJ under the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.214.01.0005.01.FRA&toc=OJ%3AL%3A2020%3A214%3ATOC.

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

- the Security Officer (security@emsa.europa.eu) and/or
- the Data Protection Officer of the Agency at: DPO@e4msa.europa.eu.

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

12. List of Attachments

- Attachment 1 - the audit report and periodic reviews *(not publicly available)*
- Attachment 2 - the map with the locations of the cameras *(not publicly available)*
- Attachment 3 - the brief technical specifications for the cameras and for the video-surveillance system as a whole including any software and hardware *(not publicly available)*
- Attachment 4 - the contract with the outsourced security company (EMSA/OP/25/2019 Lot 1, SECURITY SERVICES with Grupo 8 – Vigilância e Prevenção Electrónica, LDA - *not publicly available)*
- Attachment 5 - the template of the confidentiality undertaking
- Attachment 6 - the template of register of retention and transfers
- Attachment 7 - the Agency's on-the-spot data protection notice
- Attachment 8 - the Disclosure Request Form.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu

European Maritime Safety Agency

Attachment 5

Confidentiality undertaking

[Template]

I, [insert name and title of signatory of this declaration], the undersigned,

☐ in my own name (for a natural person)

or

☐representative of (for a request made on behalf of a legal person)

[insert name in full of the legal person, official adress in full]

Being provided with access to the video-surveillance footage and/or the technical architecture of the video-surveillance system established by EMSA, hereby confirm:

- the rights to view the footage real-time, view the recorded footage, or copy, download, delete, or alter any footage acquired by the aforementioned video-surveillance system are provided to me within the framework of my function and duties which I perform for the Agency.
- I am [and the entity that I represent and the staff proposed are] not subject to a conflict of interest in the context of the aforementioned functions and duties; a conflict of interest could arise in particular as a result of economic interests, political or national affinities, family or emotional ties, or any other relevant connection or shared interest;
- that I will inform EMSA, without delay, of any situation constituting a conflict of interest or which could give rise to a conflict of interest;
- that I will not communicate any confidential information that is revealed to me or that I have discovered. I will not make any adverse use of information given to me.
- that I will keep the footage file entrusted to me confidential. I will not disclose such a file nor the information contained in the file to any party. I will use the footage only for the purposes of my immediate function and duties in accordance with the provisions of Regulation (EC) No 45/2001of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and EMSA Video-Surveillance Rules

EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal
emsa.europa.eu

European Maritime Safety Agency

- that I [the organisation that I represent and its staff] have not sought and will not seek, have not attempted and will not attempt to obtain, and have not accepted and will not accept, any advantage, financial or in kind, from any party whatsoever, where such advantage constitutes an illegal practice or involves corruption, either directly or indirectly, inasmuch as it is an incentive or reward relating to the access rights to the video-surveillance footage and/or the technical architecture of the video-surveillance system established by EMSA.
- that I am aware that EMSA reserves the right to check this information, and I realise the possible consequences that may arise from any false declaration.

Full name and signature: Date:

European Maritime Safety Agency

Attachment 6

Register of retention and transfers

Number	Date and Time	Entity requesting the disclosure	Brief description	Justification	Deadline for EMSA copy to be destroyed	Authorised by	Signature

European Maritime Safety Agency

Attachment 7

EMSA on-the-spot data protection notice

Attachment 8
Disclosure Request Form

Event description		
Date and Time:	Location:	Report Reference:
Event type		
Theft □ Accident □ Violence/Physical aggression □ Other□ (describe)		
Brief description		
Entity requesting the disclosure		
Police□ SIS□ Other□		
Justification		
EMSA copy to be destroyed in [days]:		
Authorised by:		
Signature:		
Requested by:		
Date	Name	Signature