Video surveillance at EFSA
Implementing rules and technical specifications

PUBLIC version

1 Introduction

EFSA operates a video surveillance system (*hereafter VSS*) for the safety and security of its buildings, assets, staff and visitors. The present document and its attachments describe the EFSA's VSS and the precautions that EFSA takes to protect the personal data, privacy and other fundamental rights and legitimate interests of people filmed by the cameras.
Due to the sensitivity of the issue, the approval of the Executive Director is deemed necessary.

2 Scope

This document concerns the video surveillance system installed in the EFSA premises, Via Carlo Magno 1a, 43126 Parma as well as surveillance in representation rooms of EFSA located at Palazzo Ducale, Parma.

3 Purpose

3.1. Purpose of the video surveillance at EFSA. EFSA uses its VSS for the sole purpose of physical security and access control. The video-surveillance system helps to control the access to EFSA premises, ensuring the security and safety of premises, individuals and goods (e.g. documents, assets). It complements other physical security systems such as the access control system by means of access badges and physical intrusion control systems. It helps to prevent, deter, and if necessary, investigate unauthorised physical access and security incidents in areas under surveillance. In addition, video-surveillance helps to prevent, detect and investigate theft of equipment or assets owned by EFSA, visitors or staff and threats to the safety of visitors or staff.
This policy forms part of the broader Security Policy of EFSA, available on the Intranet Portal.

3.2. Purpose limitation. The system is not used for any other purposes than described under the previous point. Therefore, it is not used to monitor the work of individuals or their attendance or as an investigative tool (other than investigating 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 administrative inquiry, disciplinary proceeding or criminal investigation as described in point 7.5 below (see Sections 5.7, 5.8 and 10.3 of the EDPS Guidelines).

4 Ensuring efficient targeted video surveillance

4.1. Document objectives. EFSA processes the images in accordance with both the Video Surveillance Guidelines issued by the European Data Protection Supervisor (EDPS) (hereafter referred to as **'EDPS Guidelines'**) and Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies (hereafter referred to as '*the Data Protection Regulation*').

For the points listed below, the practise of EFSA derogates from the recommendations in the EDPS Guidelines. A justification is provided in the points referred to:

- Infra-red illumination – point 6.1
- Retention period of images from cameras covering limited areas outside the EFSA building perimeter – point 9

4.2. Data protection compliance

The present Policy takes account of the following:

- A data protection Audit and privacy impact analysis of the EFSA video-surveillance system was carried out in 2012. The resulting findings and recommendations have been addressed in the present Policy (see **Annex 1**);
- The EDPS Opinion following the notification for prior checking by the DPO, submitted to the EDPS in accordance with Article 27 of the Data Protection Regulation (**Annex 8**);
- Information to the Italian National Data Protection Authority.

4.3. Revision of the existing system

In order to ensure that the VSS of EFSA is compliant with the EDPS Guidelines, the system is subject to a self-audit, or anytime when substantive infrastructural changes are implemented and/or new technologies are adopted. In this case, CORSER Unit must inform the DPO and anticipate the periodical self-audit. In view of the fact that the present Policy addresses the findings and recommendations of the initial data protection audit referred to in above point 4.2, the first self-audit shall be carried out within two years after entering in force of the measures described in this document.

4.4. Decision of the Executive Director and consultation

The decision to use a video surveillance system and to adopt the safeguards described or referred to in this document was made by the Executive Director. The DPO (Data Protection Officer) and the SO (Security Officer) of EFSA have been consulted before the adoption of this document.

4.5. Transparency. There are two versions of this document: the present confidential version for restricted use and a public version available and posted on the EFSA Intranet Portal and on the EFSA official website. The public version contains summary information with respect to particular topics. Information is only omitted from the public version insofar as the preservation of confidentiality is absolutely necessary for compelling reasons in accordance with the

Regulation on public access to documents[1] (e.g. for security reasons, to preserve the confidentiality of business sensitive information, or to protect the privacy of individuals).

5 Areas under surveillance within the EFSA perimeter *(Confidential information)*

[…]

6 Collection of video images *(Confidential information)*

[…]

7 Data access and disclosure

7.1. In-house security staff and guards. Live and recorded CCTV footage is accessible to security guards on duty (contract outsourcing – see below 7.5) and EFSA staff of CORSER Unit, i.e. the head of unit and CORSER staff in charge, firstly the EFSA Security Officer and other CORSER staff in charge of office security. All persons with access to the VSS have signed a "Declaration on Confidentiality" (see **Annex 3**).

7.2. Access rights. Access credentials to the VSS are set as follows (see **Annex** 2 for details):

- A personalised administrator account for the EFSA Security Officer (+ backup), allowing granting access rights, the creation of new accounts and exporting images from the VSS;
- A personalised "super-user" account for the Security Guards Team Leader (+ backup);
- Generic user account for security guards and two staff members of CORSER Site Management Team, allowing the live viewing and viewing of recorded images;
- Generic "maintenance" account for technicians in charge of system maintenance (outsourced service)

7.3. Data protection training. The DPO organizes periodical refreshment training on data protection issues related to the VSS for all persons with access rights to the system. This data protection training is organised on a two-yearly basis. (see Section 8.2 of the EDPS Guidelines).

7.4. Confidentiality Declarations. Each individual with access to the VSS must sign the Declaration of Confidentiality (see **Annex 3** and Section 8.3 of the EDPS Guidelines). The originals of declarations are kept by the CORSER Unit in charge of the system.

7.5. Transfers and disclosures. All transfers and disclosures of CCTV footage must be formally requested in writing and documented and are subject to a rigorous assessment of the necessity for such transfer and the compatibility of the transfer with the declared security and access

[1] Regulation (EC) N° 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 31.5.2001, L145/43, article 4

control purpose (see Section 10 of the EDPS Guidelines).

- Transfers to local law enforcement authorities (e.g. *Polizia, Carabinieri*) when needed, to investigate or prosecute criminal offences

Such transfers can only be authorized following a formal written request to EFSA, signed by a sufficiently highly ranked police officer or a court order, or a similar formal request, specifying the reason why the VSS images are needed as well as the location, date and time of the requested images. Each request for disclosure to local authorities is assessed by the EFSA Security Officer (SO) and the CORSER Site Management Team and also the Data Protection Officer (DPO) may be consulted.

- Transfers to investigatory bodies of the EU and of EFSA

Transfers can be made to the European Anti-fraud Office (OLAF) in the framework of an investigation carried out by OLAF itself, by 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 and in the EFSA Implementing Rules on Administrative Inquiries and Disciplinary Proceedings, provided that it can be reasonably expected that the transfers may help the investigation or prosecution of a sufficiently serious disciplinary or criminal offence.

- Image exportation and Register of transfers

Transfers happen by exporting images from the system upon the permission of the EFSA Security Officer or on behalf of the Executive Director. Only the Security Officer, CORSER Site Management Team staff in charge and the coordinator of security guards are able to export images from the system. All transfers are registered in the **Register of retention and transfers** provided in **Annex 5** (see Sections 7.2 and 10.5 of the EDPS Guidelines).

- Outsourced service

Security surveillance with security guards is an outsourced service at EFSA. The contract between EFSA and the provider regulating this service is available as **Annex 4.**

8 Information security and data protection safeguards

A number of technical and organisational measures have been put in place in order to protect the security of the system, including personal data.

- A secure data center protected by electronic and physical access control, where the dedicated servers for storing the recorded images are hosted. EFSA's IT network infrastructure is protected against intrusion by means of firewalls ;
- Before authorised access to the system is granted, individuals concerned have been security-cleared and have signed a Declaration on Confidentiality (see **Annex 3**);
- Access rights to the system are assigned strictly on a 'need-to-know' basis to persons having access control and EFSA building security as part of their work responsibilities, i.e. the EFSA Security Officer, CORSER Site Management Team , security guards and

persons in charge of the VSS maintenance. The list of individuals having access to the system, detailing their rights, is at all times kept up-to-date.

9 Retention period of images

The images are kept for maximum 7 calendar days. For images from cameras covering limited areas outside the EFSA building perimeter as documented in **Annex 2**, the retention period is reduced to 2 working days, considered as the minimum time required for operational follow-up to security issues occurring during weekends or public holidays.
After this time period, the images are automatically overwritten on the VSS servers on a first-in, first-out basis. For images needed for further investigation purposes or to evidence a security incident, the retention period may be prolonged as long as the images are needed for this purpose. In any case, extended retention periods and transfers of VSS images are rigorously documented in the **register of retention and transfers** (see **Annex 5)** (see Section 7 of the EDPS Guidelines.). The way transfers of VSS images and related requests are handled is described in the VSS technical description (**Annex 2)**.
Once the VSS servers or other media are not longer useable, they will be safely disposed of in such a manner that the remaining data on it are permanently and irreversibly deleted.

10 Information to the public

10.1. Multi-layer approach. Information to the public about the video-surveillance is provided in an effective and comprehensive manner. To this end, a multi-layer approach is followed with a combination of the following information methods:

- On-the-spot notices to alert data subjects and the public and containing essential information about the processing in English and Italian language are placed adjacent to the areas monitored. For the limited areas outside the EFSA building perimeter captured by cameras equipped with the infra-red feature, a more extensive on-the-spot notice in Italian language is placed according to the content in **Annex 6**;
- The public version of the present Document is posted on the EFSA Intranet Portal and EFSA official website and is available within CORSER Unit upon request;
- A specific privacy statement for data subjects in the sense of Article 12 of Regulation (EC) No 45/2001 is available at the EFSA reception and with CORSER Unit – see **Annex 7**.

10.2. Specific individual notice. In addition, individuals must also be given individual notice in case they have been identified on camera provided that one or more of the following conditions apply:

- Their identity is noted in any images or recording;
- The images or recording are used against an individual;
- The images or recording are kept beyond the retention period in above point 9 and/or they are transferred in the sense of point 7.5;
- The identity of the individual is disclosed to anyone outside CORSER Unit

The provision of a notice may sometimes be delayed temporarily, for example if this is

necessary for the prevention, investigation, detection and prosecution of criminal offences[2]. The DPO is consulted in all such cases to ensure that the individual's rights are respected.

11 Data access, verification, correction and erasure

All the data subjects, including the EFSA staff and visitors and members of the public as far as captured on the VSS of EFSA, have the right to access the personal data that EFSA holds on them and correct or supplement the data. Any access request by the data subject or related requests on their personal data shall be directed to the Security Officer (e-mail: SecurityOfficer@efsa.europa.eu).
The Data Protection Officer (DataProtectionOfficer@efsa.europa.eu) may also be contacted in the event of any questions relating to the processing of personal data.

Whenever possible, the Security Officer responds to an enquiry as soon as possible and ultimately within 15 calendar days. If that is not possible, the data subject is informed on the next steps.

Where specifically requested, a viewing of the images may be arranged or the data subject may obtain a copy of the recorded images on DVD or another medium. In the event of such a request, the data subject may be asked to prove his/her identity beyond doubt (e.g. he could be asked to show the identity card when attending the viewing) and, whenever possible, also specify the date, time, location and circumstances when he/she was caught on the cameras.

A typical example of an access request by the data subject, is providing an excerpt of the CCTV footage to the bicycle owner capturing the moment of theft from the bicycle racks located in the external area of the EFSA building perimeter.

It should be added that an access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case. For example, following a case-by-case evaluation, EFSA 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 in the images, and it is not possible to acquire their consent for the disclosure of their personal data or use image editing to remedy the lack of consent.

Finally to add that in case the exercise of the data subject's rights results in the disclosure of VSS images in the way described in this section, this is documented in **the register of retention and transfers**.

12 Right of recourse

[2] Other exceptions under Article 20 of the Data Protection Regulation may also apply in exceptional circumstances.

All persons have 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 the result of the processing of their personal data by EFSA. Before doing so, EFSA recommends that they first contact:

- the Security Officer (SecurityOfficer@efsa.europa.eu), and/or
- the Data Protection Officer (DataProtectionOfficer@efsa.europa.eu);

EFSA staff members may also request a review by the appointing authority under Article 90 of the Staff Regulations.

13 Entry into force

The implementing rules described in the present document shall enter into force on the day following the date of its adoption. It repeals the previous Video surveillance policy in force since 2010. The Executive Director may review this document whenever deemed necessary.

Done at Parma 13/11/2014

Bernhard Url
Executive Director
[signed]

Annexes:

(N.B. considered confidential except for Annexes 6-7)

- **Annex 1:** Data Protection Audit and Privacy Impact Assessment (2012);
- **Annex 2:** Video Surveillance System technical description;
- **Annex 3:** Model for the Confidentiality Declarations (Section 8.3 of the EDPS Guidelines);
- **Annex 4:** Contract with the outsourced security company *I.V.R.I.*;
- **Annex 5:** Register of retention and transfers (point 10.5 and 7.2 of the EDPS Guidelines);
- **Annex 6:** On-the-spot CCTV data protection notices of EFSA;
- **Annex 7:** Specific Privacy Statement for data subjects;
- **Annex 8** EDPS opinion on EFSA VSS-16 July 2013
- **Annex 9** Extract from EFSA Security Assessment – EU - JRC_28/03/2014.