Data protection notice for EFCA's video-surveillance system

1. What areas are under surveillance?

The video-surveillance system consists of a set of fixed and mobile cameras. Fixed cameras are located at the entrance of each floor, the conference room, the external roof terraces and the UPS and Diesel Generator rooms. Mobile cameras are located at entry and exit points of our building, including the main entrance, and the garage. There are no cameras elsewhere either in the building or outside of it, eg. there are no cameras located in individual offices.

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

EFCA's video-surveillance system is used for the safety and security of its buildings, assets, staff and visitors and is necessary for the management and functioning of the Agency (Article 5(a) and recital 27 of the Regulation (EC) No 45/2001).

3. What personal information do we collect and for what purpose?

The video-surveillance system is a conventional static system equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. The image quality in most cases allows your identification if you are in the camera's area of coverage.

Cameras are fixed and cannot be used by operators to zoom in on a target or follow individuals around. An exception in this regard exists for some of the cameras used for the control of the main entrance of the building and the garage.

The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to our building and helps ensure the security of our building, the safety of our 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 taken to 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 or threats to the safety of personnel working at the office (e.g. fire, physical assault).

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. The system is also not used as an investigative tool or to obtain evidence, unless a security incident is involved. 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 4 below.

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

Recorded video is accessible to our in-house security staff only (namely the Local Security Officer and the Logistics Officer). Live video is also accessible to security guards on duty and to a limited extent to reception staff. These security guards and the reception staff work for out-sourced companies.

All transfers 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 DPO of the Agency is consulted in each case of transfer.

No access is given to management[1] or human resources except when necessary within the meaning of the purpose as mentioned in Section 3 above.

Subject to the case by case analysis, and considering also the initial purposes of the recording, national police, courts, or other national authorities may, in some cases, also be given access to video-surveillance footage if needed to investigate or prosecute criminal offences.

Under exceptional circumstances, and subject to the procedural safeguards noted above, access may also be given European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF and 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.

5. How do we protect and safeguard your information?

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organizational measures have been put in place. 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. All staff with access rights (external and internal) sign a confidentiality undertaking.

Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs. Only the in-house security staff, following communication to the DPO, is entitled to grant, alter or annul access rights of any person.

6. How long do we keep your data?

Recorded video-surveillance data is retained for a maximum of 7 calendar days. Thereafter, all images are overwritten and consequently deleted. If any image needs to be stored as evidence or to further investigate a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed.

7. How can you verify, modify or delete your information?

You have the right to access the personal data we hold regarding you and to correct and complete them. Any request for access, rectification, blocking and/or erasing of personal data should be directed to Mr. Niall McHale, Head of Unit Resources niall.mchale@efca.europa.eu. You may also contact him in case of any other questions relating to the processing of personal data.

Whenever possible, the in-house security staff will respond to your enquiry in substance within 15 calendar days. If this is not possible, you will be informed within this time informed of the reason for the delay and the next steps. Even in the most complex cases, you will be granted access or

[1] Excluding the Head of Unit Resources acting in his capacity as Local Security Officer.

receive a final reasoned response for the rejection of your request within one month at the latest. Any response will be given as soon as possible, especially if you establish the urgency of the request.

If you specifically request, a viewing of your images may be arranged or you may obtain a copy of your recorded images on a DVD or other customary support. In case of such a request, please indicate your identity beyond doubt (e.g. you may bring your identity card when present yourself for the viewing) and also designate the date, time, location and circumstances when you were caught on cameras. Please also provide a recent photograph that allows the security staff to identify you from the images reviewed.

At this time, we do not charge you for requesting a viewing or a copy of your recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

Please also note that we cannot always provide you with an image as exemptions under Article 20(1) of Regulation 45/2001 may apply. For example, upon a case-by case evaluation we may have to conclude that restricting your 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.

8. What is our compliance status with applicable data protection laws?

The Agency processes your images in accordance with the Video-Surveillance Guidelines issued by the European Data Protection Supervisor (http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines) and Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies. Considering the limited scope of the system, it was not necessary to submit a prior checking notification to the EDPS but we notified him of our compliance status by sending him a copy of our video-surveillance policy. A periodic data protection review is undertaken by logistics every two years.

9. Right of recourse

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation 45/2001 have been infringed as a result of the processing of your personal data by the Agency. Before doing so, we recommend that you first try to obtain recourse by contacting the:

- EFCA's Head of Unit Resources, and/or
- EFCA's Data Protection Officer[2]

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

[2] Rieke ARNDT, rieke.arndt@efca.europa.eu