EUROPEAN DEFENCE AGENCY

DECISION N° 12/27

of 21 December 2012

adopting an EDA Video-surveillance Policy

THE CHIEF EXECUTIVE,

Having regard Council Decision 2011/411/CFSP of 12 July 2011 defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP, notably to Article 10 thereof,

HAS DECIDED AS FOLLOWS:

Article 1

The EDA Video-surveillance Policy annexed hereto is hereby adopted.

Article 2

The "European Defence Agency CCTV System Policy", dated 10 June 2009, is hereby repealed.

Article 3

This decision shall enter into force on the date of its adoption.

Done at Brussels, on 21 December 2012.

Claude-France Arnould
Chief Executive

Annex I

EDA Video-surveillance Policy

Adopted by the EDA Chief Executive's Decision on 21 December 2012

1. Purpose and scope of the Agency's Video-surveillance Policy

For the safety and security of its buildings, assets, staff and visitors, our Agency operates a video-surveillance system. This 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 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. Revision of the existing system. A video-surveillance system had already been operating in our Agency before the issuance of the Video-Surveillance Guidelines by the European Data Protection Supervisor ("**Guidelines**"). Our procedures, however, have since then been revised to comply with the recommendations set forth in the Guidelines[1].

2.2. 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.

2.3. Self-audit. The system has been subject to a fact-finding exercise. The report can be found attached as **Attachment 1.** A self-audit of the system with the involvement of the EDA internal auditor is scheduled to be held before the end of 2012.

2.4. 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 (Guidelines, Section 3.2) or to submit a prior checking notification to the EDPS (Guidelines, Section 4.3).

When adopting this Video-surveillance Policy, we simultaneously notified the EDPS of our compliance status by sending them a copy of our Video-surveillance Policy and our first fact-finding exercise report.

2.5. Contacts with the relevant data protection authority in the Member State.
The competent data protection authority in Belgium was informed and its concerns and recommendations were taken into account.

2.6. Chief Executive'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 Chief Executive of the Agency after consulting:

- the Head of the Agency's Security Unit,
- the Agency's Data Protection Officer,
- and the Staff Committee.

[1] The Guidelines are available at the EDPS website dated on march 2010 retrieved on : http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf.

During this decision-making process, the Agency

- demonstrated and documented the need for a video-surveillance system as proposed in this policy,
- discussed alternatives and concluded that the maintenance of 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.

2.7 Transparency. The EDA Video-surveillance Policy has two versions, a version for restricted use and a public version available and posted on our intranet sites at **[http://intranet/DP/SitePages/Home.aspx]**. The public version of the Video-surveillance Policy may contain summary information with respect to particular topics or attachments. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons[2].

2.8. Periodic reviews. A periodic data protection review will be undertaken by the EDA Security Unit every two years, the first by 31 December 2014. 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). Copies of the periodic reports will also be attached to this Video-surveillance Policy in **Attachment 1**.

3. What areas are under surveillance?

The EDA video-surveillance system comprises a number of cameras around our premises. They are located at entry and exit points of our building, including the main entrance, emergency and fire exits and the entrance to the parking lot. In addition, there are also cameras to protect sensitive areas.

We do not monitor any 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 minimize the monitoring of areas that are not relevant for the intended purposes.

Monitoring outside our building on the territory of Belgium is limited to an absolute minimum, as recommended in Section 6.5 of the Guidelines.

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

4.1. Summary description and detailed technical specifications for the system.

[2] The restricted version of this policy includes the attachments recommended in the EDPS video surveillance guidelines, which for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals, are not included in the public version. The restricted version is available to EDA Staff and EDPS inspectors.

The video-surveillance system is a conventional static 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 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage.

The cameras are all fixed (there are no pan-tilt-and-zoom cameras), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around.

We do not use high-tech or intelligent video-surveillance technology, do not interconnect our system with other systems, and we do not use covert surveillance, sound recording, or "talking CCTV". The technical specifications for the cameras and for the video-surveillance system as a whole 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 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 to support our 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 (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 6.5 below.

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

4.5. Webcams. We have no webcams.

4.6. No special categories of data collected. We collect no special categories of data.

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 our Agency (for the security and access control purpose described in Section 4.2 above). Therefore, we have a lawful ground for the video-surveillance. A more detailed and specific legal basis for the video-surveillance is provided in this Video-surveillance Policy. This policy, in turn, forms part of the broader security policies adopted by our Agency.

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

6.1. In-house security staff and outsourced security-guards. Recorded video is accessible to our in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an out-sourced security company.

In **Attachment 2** is included the summary of video-surveillance measures followed by the outsourced security company. The **contract with this security company** is included as well in this attachment in the restricted version.

6.2. Access rights. The Agency's Security Policy for Video-surveillance (see Section 7 below and Attachment 7 clearly specifies and documents 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 document specifies who has 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 outsourced security guards, have received a data protection training either by the EDA Data Protection Officer or the outsourced security company.

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

6.4. Confidentiality undertakings. After the training each staff member also signed a confidentiality undertaking. This undertaking was also signed by the outsourced company. Copies of these **confidentiality undertakings** are part of Attachment 5, and available for EDA Staff to be consulted in the EDA Security Office, upon requirement.

6.5. Transfers and disclosures. All transfers and disclosures outside the security unit 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.

EDA Security Office, following instructions by EDA Chief Executive as Agency Appointing Authority and Security Authority, may carry out internal investigations in the cases, for the purposes and objectives described in article 138 of current EDA Staff Regulations and article 15, point 2 (d) of Council Decision 2011/292/EU.

The register of retention and transfers is included in **Attachment 6**. The DPO of the Agency is consulted in each case.

No access is given to management or human resources.

Local police may be given access if needed to investigate or prosecute criminal offences.

Under exceptional circumstances, to be specifically approved by EDA Chief Executive, access may also be given to:

- *the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF, 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. No requests for data mining are

accommodated. Since the entry into force of this policy, we have not authorised a transfer under any of the above grounds.

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. These are detailed in a processing-specific security policy ("**Security Policy for Video-surveillance**"), which is attached as **Attachment 7**.

The Agency's Security Policy for Video-surveillance was established in accordance with Section 9 of the EDPS Video-surveillance Guidelines.

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 outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared.
- All staff (external and internal) signed non-disclosure and confidentiality agreements.
- 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 Security Policy for Video-surveillance (see Attachment 7).
- The Security Unit of EDA keeps an up-to-date list of all persons having access to the system at all times. A detailed description of the applicable access rights is included.

8. How long do we keep the data?

The images are retained for a maximum of 1 month[3]. 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. 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 security control room annexed to the ground floor reception, 24 hours a day.

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, we follow a multi-layer approach, which consists of a combination of the following two methods:

[3] The justification on the maximum retention period for registered images, adopted by EDA is explained in the second paragraph of the point "data storage security procedures" of the "Security policy for video surveillance" (Attachment 7)

- 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,

- we post this Video-surveillance Policy on our intranet sites for those wishing to know more about the video-surveillance practices of our Agency.

- Print-outs of this Video-surveillance Policy are also available at our reception desk and from our security unit upon request. Two email addresses are provided for further enquiries: dpo@eda.europa.eu; security@eda.europa.eu. Also the following telephone number +32 (0)25042801.

We also provide on-the-spot notice adjacent to the areas monitored. We placed some notices near in all entrances, including the entry to the parking lot, and some other places.

The Agency's on-the-spot data protection notice is included as **Attachment 8.**

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 security unit, *or*

- if 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 offences. The Institution'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 the EDA Head of Security Unit (security@eda.europa.eu) (+32 (0)25042801). He or she may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the EDA Security Unit 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 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 20(1) of Regulation 45/2001 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.

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, we recommend that individuals first try to obtain recourse by contacting:

- the Head of the EDA Security Unit (see contact details above), and/or
- the Data Protection Officer of the Agency (dpo@eda.europa.eu)
- Staff members may also request a review from their appointing authority under corresponding articles of EDA Staff Regulation.

Attachments to the Video-surveillance Policy:

- **The fact-finding exercise report** is attached as **Attachment 1.** Attachment 1 will also contain the first self-audit and the **periodic reviews.**
- A list with the **locations of the cameras** is included in **Attachment 2** (in the restricted version).
- The **technical specifications** of the cameras and of the video-surveillance system as a whole are included in **Attachment 3**.
- In **Attachment 4** it is included the summary of video-surveillance measures agreed with the outsourced security company**.** The **contract with this security company** is also included in the restricted version of this attachment.
- Copies of the **confidentiality undertakings** are attached as **Attachment 5** (available in the register version).
- **The register of retention and transfers** is included in **Attachment 6**
- In order to protect the security of the video-surveillance system, including personal data contained in it, a number of technical and organizational measures have been put in place. These are detailed in a processing-specific security policy ("**Security Policy for Video-surveillance**"), which is attached as **Attachment 7**.
- The Agency's **on-the-spot data protection notice** is included as **Attachment 8.**

ATTACHMENT 1

EDA FACT-FINDING EXERCISE REPORT

ON VIDEO-SURVEILLANCE PRACTICES

IN ACCORDANCE WITH DATA PROTECTION

The scope of the Regulation and Video surveillance guidelines covers in our Agency exclusively our permanent video-surveillance security systems. The guidelines do not apply to our video-conferencing systems, cameras of Media and Communication Unit, cameras used for training activities, etc.

Existing EDA practices on Video Surveillance, to a large extent, already follow the recommendations in the Guidelines, and therefore, for the most part, all we need to know is to verify and confirm this in writing. Some aspects have been identified, which require specific adjustments to further improve our level of compliance. In this respect, here are some identified targets:

1. The video-surveillance system in EDA is a conventional static 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 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage. The cameras are all fixed (except 2 pan-tilt cameras which can be moved at distance, although they act like the fixed ones), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around. We do not use high-tech or intelligent video-surveillance technology, do not interconnect our system with other systems, and we do not use covert surveillance, sound recording, or "talking CCTV".

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

3. The obligations of the processor with respect to data protection must be clarified in writing and in a legally binding manner. Our contract with the outsourced security company should cover this. In particular, its obligation with regard to confidentiality of the data processed, and to provide appropriate training to its staff, including on data protection.

4. The location of the cameras ensure that the video-surveillance is the less intrusive possible to the privacy of staff and visitors, since they are strategically situated for ensuring access control to the premises, and to strategic locations, as some archives and security areas.

5. Our Agency has a Video Surveillance Policy, but an update is needed.

6. A formal audit is also needed, to be followed up every 2 years. The internal auditor has been approached and agreed to conduct an audit in coordination with the Data Protection Officer, by the end of 2012. According to the guidelines, EDA should not rule out the possibility of a third party audit.

7. In this respect, the EDPS recommends internal auditors to receive adequate training on data protection and the guidelines. Also training is mandatory for all EDA Staff personnel with access rights to the system, and for the outsourced security guards.

8. All the above mentioned Staff managing the system need to sign a confidentiality undertaking.

9. A register of retention and transfer exists in accordance with the guidelines.

10. DPO should notify the EDPS about the compliance status of the Agency, just after every formal audit.

11. To better guarantee fair processing of data, first steps have been taken to make the policy available to the public. Also the Agency's on-the-spot data protection notice to Staff and visitors to our premises is properly placed in accordance with the Video Surveillance Guidelines.

12. As the current EDA Video Surveillance Policy is limited to Staff, a second version available to the public is going to be produced and posted on our intranet sites, and made available to the public, instead of the current restricted in use.

13. It has been checked that the guards from the outsourced security company in fact are operating the system in accordance with the current Video-surveillance Policy.

14. In our Video Surveillance Policy the period of time for which the recordings will be retained should be specified. Currently, footage is automatically deleted after 1 month, which is in accordance with the Host Nation's Law. The regulation in this respect mentions that "recordings must not be retained longer than necessary". On the other hand, the Guidelines recommend the period for typical security purposes to be one week.

14/06/2012

[signed]

EDA Head of Security

ATTACHMENT 2

LIST WITH THE LOCATIONS OF THE CAMERAS

(available in the restricted version)

ATTACHMENT 3

TECHNICAL SPECIFICATIONS OF THE CAMERAS

AND THE SYSTEM AS A WHOLE

(available in the restricted version)

ATTACHMENT 4

SUMMARY OF VIDEO-SURVEILLANCE MEASURES

AGREED WITH THE OUTSOURCED SECURITY COMPANY[4]

The contractor, as processor of the EDA video-surveillance system, compromises to

comply with the provisions of

- the Regulation 45/2001 on the protection of personal data by Community institutions and bodies, (the Regulation),
- the EDPS Video-Surveillance Guidelines of 10 march 2012 (the Guidelines),
- the EDA's Video-surveillance Policy, and,
- with any further advice given by the EDPS, for example, in an eventual prior checking or complaint procedure or as a result of an inspection or consultation.

In particular,

The security guards working in the EDA control room are technically allowed to view footage real-time and operate the cameras (e.g. zoom on an object), or view recorded footage on-line, but they are not given technical access to features such as copying, downloading, deleting, or altering any footage.

In addition, while the guards are expected to monitor the footage real time and operate the cameras as necessary to perform their monitoring tasks, they should be instructed not to use the cameras to zoom in on a target, for example, a group of people peacefully demonstrating in front of the building, or two staff members passing by, if this is not necessary to ensure the security and access control purpose for which the monitoring is carried out.

All personnel with access rights, including those carrying out the day-to-day CCTV operations or the maintenance of the system, should be given data protection training and should be familiar with the provisions of the Guidelines in so much as these are relevant to their tasks. The training should pay special attention to the need to prevent the disclosure of video-surveillance footage to anyone other than authorized individuals.

Any possible direct or indirect subcontractor must be bound by the same obligations as the direct contractor. EDA reserves the right to veto the choice of subcontractor, if reasonable doubts arise regarding its ability to comply with the data protection requirements.

The EDA Security Unit, remains liable for compliance with the Regulation as the "data controller", thus, it will ensure that the security guards carry out their activities in compliance with the provisions of the

[4] The Contract with the Security Company is included in the restricted version of this attachment.

Regulation and the Guidelines. Whenever deemed necessary, it could also provide appropriate training to the contractor's Staff with access to the footage.

After receiving the training on video-surveillance, the contractor personnel will sign confidentiality undertakings to ensure that they will not transfer, show, or otherwise disclose the content of any video-surveillance footage to anyone except authorised recipients.

ATTACHMENT 5

CONFIDENTIALITY UNDERTAKINGS

(available in the restricted version)

ATTACHMENT 6

REGISTER OF RETENTION AND TRANSFERS

EDA Security Unit keeps a register in an electronic form – of transfers and disclosures. In it, each transfer to a third party (any transfer outside the Security Unit) will be recorded.

The register, in addition, will contain all instances where, although the copy of the video-surveillance footage was not transferred, third parties were shown the recordings or when the content of the recordings was otherwise disclosed to third parties.

The register includes the following:

- the date of the recordings,
- the requesting party (name, title and organisation),
- the name and title of the person authorising the transfer,
- a brief description of the content of the recordings,
- the reason for the request and the reason for granting it, and finally,
- whether a copy of the footage was transferred, the footage was shown, or verbal information was given.

ATTACHMENT 7

SECURITY POLICY FOR VIDEO SURVEILLANCE

The servers storing the images recorded by the EDA video-surveillance system are inside the booth at the reception desk of the Agency. They are secured since there are outsourced security personnel next to them 24 hours a day, every day of the year. Furthermore, all our premises are protected by physical security measures following the strictest rules. The system itself is isolated, and thus, not connected to any other network. The main computer systems holding the data are security hardened, and have firewalls and other IT security software to protect the data contained.

Administrative measures include the obligation of all outsourced personnel having access to the system:

- The system (live video mode) is operated by Staff of our current outsourced security contractor.
- The recorded footage is managed exclusively by EDA Staff, who are in possession of a EU Personnel Security Clearance at least at level CONFIDENTIAL.
- The maintenance of the equipment and system as a whole has been as well externalized to another company (also well recognized in the field of Security by our Host Nation, Belgium).

- All staff (external and internal) signed non-disclosure and confidentiality agreements, after being briefed in Data Protection according to the EDPS guidelines on video-surveillance.
- Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
- Only the system administrator (the maintenance contractor) specifically appointed by the controller for this purpose (EDA Security Unit) is able to grant, alter or annul access rights of any persons.
- In the EDA Security Office there is an up-to-date list of all persons having access to the system at all times.

In the following lines you can find the description of the most important security measures applied to safeguard personal data:

<u>Operation of the system</u>

The Operations will be administered and managed by the EDA Security Unit in accordance with the principles and objectives expressed in the Agency's Video-surveillance Policy.

The day-to-day management will be the responsibility of the Security Unit in cooperation with the security service provider during the day and out of working hours and weekends.

The Security Control Room will only be staffed by the staff employed by the security service provider.

The CCTV system will be operated 24 hours each day, every day of the year.

Security Control Room

The Control Room 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.

Unless an immediate response to events is required, staff in the Security Control Room must not direct cameras at an individual or a specific group of individuals.

Access to the Security Control Room will be strictly limited.

The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted.

Visitors must first obtain permission from the Head of Security Unit of the Agency and must be accompanied by at least one Security Unit staff member throughout the visit.

Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

Control Room 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 Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.

A 'feuille de rapport' (register of retention and transfers) will be maintained in the Control Room and electronically in the EDA Security Unit. Full details of visitors including time/data of entry and exit will be recorded.

There must always be at least one Control Room Operator present within the Control Room.

Data storage security procedures

The images are retained for a maximum of 1 month. Thereafter, all images are deleted. If any images needs to be stored to further investigate or evidence a security incident, they may be retained as necessary.

The retention period is justified because; based on the experiences regarding access needs to registered images for security purposes, EDA is clearly not able to assure its security mission, especially regarding protection of European Union classified information (EUCI), as set out in the Council Decision 2011/292/EU, should the retention period of registered images is due to be kept for a period shorter than thirty (30) days. Indeed, between a security incident regarding protection of EUCI

takes place, it is acknowledged by the Security Office and until the decision to view the registered images is established, it could take 2-3 weeks minimum. For the aforementioned reasons and based on the procedures of many EDA participating member states, including the host nation, EDA has decided for a realistic retention period, in consideration of its objectives, video-surveillance means and direct relation with its needs.

In order to maintain and preserve the integrity of the data recorded at the events and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

(i) Each media must be identified by a unique mark.

(ii) Before using each media must be cleaned of any previous recording (if the media is rewritable).

(iii) Staff from the EDA Security Unit shall register the date and time of media insert, including media reference.

(iv) 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 Head of the Security Unit, dated and returned to the evidence data store.

(v) If the media is archived the reference must be noted.

Data may be viewed by the Police for the prevention and detection of crime, authorized display and training.

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 'feuille de rapport' (register of retention and transfers) and need prior approval of the Head of Security Unit.

Should data be required as evidence, a copy may be released to the Police under the procedures described in the Agency's Video-surveillance Policy.

Media will only be released to the Police on the clear understanding that the Media remains the property of the EDA, and both the Media and information contained on it are to be treated in accordance with this Policy. The EDA 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 EDA 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.

Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Head of Security Unit. In these circumstances media will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

Breaches of the policy (including breaches of security)

Any breach of the CCTV Policy by staff will be investigated by Agency's Security Unit, in order for them to take the appropriate action.

ATTACHMENT 8

AGENCY'S ON-THE-SPOT DATA PROTECTION NOTICE

FOR YOUR SAFETY AND SECURITY

This building and its immediate vicinity is under video-surveillance. All cameras operate 24 hours a day, seven days a week.

The recordings are retained like precised in the EDPS video-surveillance guidelines.

For further information, please consult our Video-surveillance Policy on our intranet site :

http://intranet/Security/Document%20Library/EDA%20CCTV%20System%20policy.pdf

OR

contact the Agency's security unit at 02/504.28.01 - security@eda.europa.eu