Video-surveillance Policy

PO.FACI.001-1

	Post	Signature	Date
Prepared by:	Deputy Director	- original signed -	21/07/2015
Quality reviewed by:	Quality Management Officer	- original signed -	11/06/2015
Verified by:	Data Protection Officer	- original signed -	11/06/2015
Verified by:	Staff Committee	- original signed -	18/06/2015
Verified by:	Deputy Director	- original signed -	21/07/2015
Approved by:	Director	- original signed -	22/06/2015

DOCUMENT CONTROL SHEET

Process area Support processes

Main process Facility Management

Main process owner Head of Corporate Services Department

TABLE OF CONTENT

Abbreviations

CCTV	Closed circuit television system
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
HR	Human Resources
ICT	Information and Communication Technology
OLAF	European Anti-Fraud Office

Definitions

Data mining	Process of extrapolating patterns from existing databases
Personal data	Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity
Video-surveillance	Monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring

LOG OF ISSUES

Issue	Issue date	Change description
001	21/07/2015	First issue

1. INTRODUCTION

For the safety and security of its staff, visitors, buildings, assets and information, and for logistical reasons, CEPOL operates a video-surveillance system on parts of its premises.

2. SCOPE

This policy describes the CEPOL's video system and the safeguards the protection of personal data, privacy and other fundamental rights and legitimate interests of individuals viewed by the cameras.

This policy does not apply to the recording or broadcasting of events for the purposes of the press and public communication.

3. COMPLIANCE WITH RELEVANT DATA PROTECTION LAW

CEPOL operates its video systems in compliance with Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data. In so doing, it has due regard for the recommendations set out in the Video-surveillance Guidelines (https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf) issued by the European Data Protection Supervisor (the 'Guidelines') of 17 March 2010.

The use of the video system is necessary for the good management and functioning of CEPOL.

The CEPOL video system is subject to notification to the CEPOL Data Protection Officer (DPO) in accordance with Article 25 of Regulation (EC) No 45/2001, and to the European Data Protection Supervisor (EDPS).

The Video-surveillance Policy shall be available on the CEPOL website www.cepol.europa.eu.

To enhance the protection of privacy, CEPOL has provided for:

a) limitation of storage times of footage in line with security requirements, and
b) strict management of operators' rights regarding access to the closed circuit television system ('CCTV').

4. AREAS MONITORED

The location of the cameras has been carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes. Monitoring outside the CEPOL building on the territory of Hungary is limited to an absolute minimum.

CEPOL does not monitor areas under heightened expectations of privacy, such as offices or social areas.

5. PERSONAL DATA COLLECTED AND ITS PURPOSE

The video system is a conventional system. It records digital images and is equipped with motion detection. It records defined movement detected by the cameras in the monitored area, together with the time, date and location. All cameras can be operated twenty-four hours a day (depending on the CEPOL needs), seven days a week. When necessary, the image quality of certain cameras allows identification of individuals in the camera's area of coverage.

Purpose of using the video system

CEPOL uses its video system for the sole purposes of security and safety. The video system helps ensure the security of CEPOL premises, the safety of staff and visitors, as well as property and information located or stored on the premises.

When necessary, it complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support broader security policies on the security rules for protecting EU classified information 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.

Purpose limitation

The system is not used for any other purpose, such as to monitor the work of staff, 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. These are conducted always under a specific mandate of the Appointing Authority and in consultation with the CEPOL DPO, as appropriate.

***Ad hoc* video use and transfers**

Where there is a duly justified security need for *ad hoc* video-surveillance, such operations are planned beforehand, an impact assessment is drawn up and under a specific mandate of the Appointing Authority and in consultation with the CEPOL DPO.

Prior to making an a*d hoc* transfer, CEPOL DPO shall be consulted with.

Webcams

CEPOL does not use webcams for video-surveillance purposes.

Special categories of data

CEPOL's video system does not aim at capturing or otherwise processing images which reveal so-called 'special categories of data' within the meaning of Section 6.7 of the Guidelines.

6. ACCESS TO THE PERSONAL DATA COLLECTED

The CEPOL's Security Policy for Video-surveillance 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.

Access to recorded and live video is limited to the Security Officer on a need-to-know basis.

Access to the footage and/or the technical architecture of the video system is limited to the Security Officer on a need-to-know basis. No access rights are given to anyone other than in-house and outsourced security personnel and those responsible for the technical maintenance of the system.

Training

All personnel with access rights, including the outsourced security guards, were 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.

After the training each staff member signs a confidentiality undertaking. This undertaking is also signed by all external subcontractors and their personnel.

Transfers and disclosures

All transfers and disclosures outside the Security Officer's office are documented and subject to a rigorous assessment of the need for such a transfer and the compatibility of the purposes of the transfer with the initial security purpose of the processing.

The register of retention and transfers is maintained by the Security Officer. The CEPOL DPO is informed in each case.

No access is given to management or human resources, except in the framework of disciplinary procedures directly triggered by a physical security incident and under a mandate from the Appointing Authority.
Under exceptional circumstances, access may also be given to

a) the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF,

b) 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

c) those carrying out a formal internal investigation or disciplinary procedure within CEPOL,

d) 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.

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

No requests for data mining are accommodated.

Any breach of security regarding cameras is indicated in the register and the CEPOL DPO is informed without delay.

7. PROTECTING AND SAFEGUARDING PERSONAL DATA

In order to protect the security of the video system, including personal data, the following technical and organisational measures have been put in place:

7.1 Secure premises, protected by physical security measures, host the servers storing the recorded images; the video-surveillance IT system is a standalone one, not interconnected to any other IT system.

7.2 Administrative measures include the obligation of all personnel with access to the system (including those maintaining the equipment and the systems) to be individually security checked and cleared.

7.3 All staff sign non-disclosure and confidentiality agreements.

7.4 Access rights to users are granted to only those resources which are strictly necessary to carry out their duties.

7.5 Only the Security Officer, specifically appointed by the Director for this purpose, is able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to strict criteria.

7.1 The plans to install or update a video-surveillance system should be communicated to the CEPOL DPO. The CEPOL DPO should be consulted in all cases and should be involved in all stages of the decision-making.

7.2 Personal data processing is subject to periodic reviews (every 2 years, and also every time a significant change is planned, e.g. significant system upgrade) by the ICT function in collaboration with the CEPOL DPO and the CEPOL Internal Control Officer, to verify compliance with Regulation (EC) No 45/2001 and the EDPS Video-surveillance Guidelines.

CEPOL Video-surveillance Policy has been drawn up in accordance with Section 9 of the EDPS Guidelines.

8. DURATION OF DATA RETENTION

The images are retained for 1 week. Thereafter, images are deleted according to the 'first- in-first-out' principle. If a security incident occurs, the relevant footage may be retained beyond the normal retention periods for as long as it is necessary to further investigate the security incident.

Retention is rigorously documented and the need for retention is periodically reviewed. The register of retention and transfers is maintained by the Security Officer, and may be consulted by the EDPS, the Internal Control Officer of CEPOL and the CEPOL DPO.

9. INFORMATION TO THE PUBLIC

General information:

9.1 on-the-spot pictogram notices are posted throughout the CEPOL premises to alert the public to the fact that monitoring takes place, and

9.2 the Video-surveillance Policy is posted on the CEPOL internet site and for those wishing to know more about the video practices of the Agency.

9.3 Information hand-outs are also available at our reception desks and from the Security Guards upon request. Information is provided for further enquiries.

9.4 Notices are affixed adjacent to the entrances to CEPOL premises.

9.5 CEPOL information hand-outs and on-the-spot notice is included in the Annex.

Specific individual notice

Notwithstanding the rules applicable to investigations, individuals must also be given individual notice if they are identified on camera (for example, by Security Officer in a security investigation) provided that one or more of the following conditions also applies:

a) their identity is noted in any files/records,

b) the video recording is used against the individual, kept beyond the regular retention period or transferred outside the Security Officer's office, or

c) if the identity of the individual is disclosed to anyone outside the Security Officer's office.

Provision of notice may be delayed if it is necessary for preventing, investigating, detecting and prosecuting criminal offences, as provided for in Article 20 of Regulation (EC) No 45/2001.

CEPOL DPO is consulted in all such cases to ensure that the individual's rights are respected. Provisions of notice may sometimes be delayed temporarily, for example, if it is necessary for prevention, investigation, detection and prosecution of criminal offences. If such situation arises, please seek advice from the CEPOL DPO (dpo@cepol.europa.eu).

Access requests by the general public

Members of the public have the right to access the personal data CEPOL 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 Data Controller, CEPOL's Security Officer (security@cepol.europa.eu). The Data Controller may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the Security Officer responds to an enquiry in substance within 15 working days. An access request may be refused when an exemption under Article 20(1) of Regulation (EC) No 45/2001 applies in a specific case.

Access to the minimum information required under Article 13 of the Regulation (EC) No 45/2001 is provided free of charge.

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 (EC) No 45/2001 have been infringed as a result of the processing of their personal data by CEPOL. Before doing so, it is recommended that individuals first try to obtain recourse by contacting:

a) the Data Controller (security@cepol.europa.eu), and/or

b) the CEPOL DPO (dpo@cepol.europa.eu).

Staff members may also request a review from the Appointing Authority under Article 90 of the Staff Regulation.

ANNEX 1: ON THE SPOT HAND-OUT

For your safety and security, these premises are under video-surveillance. Images are recorded. The recordings are retained for 7 days.

CEPOL processes your images in accordance 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 (OJ L 8, 12/01/2001).

CEPOL's Video-surveillance Policy is accessible online at www.cepol.europa.eu. The EDPS' Video-surveillance Guidelines are accessible online at https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines

Data Subjects can request to verify, modify or delete their information, address further questions and obtain information on how to obtain recourse in-house by contacting the Data Controller, CEPOL's Head of Corporate Services Department (security@cepol.europa.eu).

Access to the minimum information required under Article 13 of the Regulation (EC) No 45/2001 is provided free of charge.

Data Subjects have the right to recourse to the European Data Protection Supervisor at any time (www.edps.europa.eu).

* * *

Biztonsága érdekében ez egy biztonsági kamerák által megfigyelt terület. A képeket rögzítjük és a felvételeket 7 napig tároljuk.

Amennyiben további információra lenne szüksége forduljon a CEPOL Biztonsági Részlegéhez (security@cepol.europa.eu; +36 (0) 1 803 8020).

A CEPOL a videófelvételeket az EU (EC) 45/2001 sz. Europai Únios Szabályzat alapján kezeli, amely szabályzat az úniós intézményeknél és szerveknél érvényes személyes adatok védelméről szól (OJ L 8, 12/01/2001).

ANNEX 2: ON THE SPOT NOTICE

For your safety and security, these premises are under video-surveillance. Images are recorded. The recordings are retained for 7 days.

For further information please contact CEPOL's Security Sector (security@cepol.europa.eu; +36 (0) 1 803 8020).

CEPOL processes your images in accordance with Community Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies (OJ L 8, 12/01/2001).

* * *

Biztonsága érdekében ez egy biztonsági kamerák által megfigyelt terület. A képeket rögzítjük és a felvételeket 7 napig tároljuk.

Amennyiben további információra lenne szüksége forduljon a CEPOL Biztonsági Részlegéhez (security@cepol.europa.eu; +36 (0) 1 803 8020).

A CEPOL a videófelvételeket az EU (EC) 45/2001 sz. Europai Únios Szabályzat alapján kezeli, amely szabályzat az úniós intézményeknél és szerveknél érvényes személyes adatok védelméről szól (OJ L 8, 12/01/2001).