Opinion on the notification for prior checking received from the Data Protection Officer ("DPO") of the European Anti-Fraud Office ("OLAF") on 17 October 2007 regarding OLAF's CCTV system

Brussels, 19 May 2008 (Case 2007-634)

1. Proceedings

On 17 October 2007 OLAF's DPO submitted a notification for prior checking to the European Data Protection Supervisor ("**EDPS**") about OLAF's planned data processing operations related to its newly installed CCTV system ("**Notification**").

On 24 November 2007 the EDPS requested additional preliminary information from OLAF. OLAF's DPO replied on 26 November 2007. On the same day, the EDPS requested further information. OLAF replied on 28 November. On the same day, the EDPS sent to OLAF a third set of questions requesting further information.

On 7 December 2007 OLAF sent to the EDPS an updated version of its Notification. The EDPS complemented his previous information requests and sent to OLAF a final, fourth set of questions on the same day. OLAF responded to the remaining EDPS questions (third and fourth set of questions) on 13 March 2008.

On 3 April 2008, the EDPS sent to OLAF's DPO a summary of his understanding of the facts, to ensure the accuracy of the information received from OLAF. Until OLAF's final written confirmation of the facts on 17 April 2008, the case remained suspended.

Finally, the procedure was suspended for 29 days between 17 April 2008 and 16 May 2008 during which OLAF commented on the draft EDPS Opinion.

2. The facts

2.1. Scope of the Notification. The Commission building which houses OLAF is equipped with two CCTV systems:

- OLAF's CCTV system, which covers only the OLAF secure premises; and
- the Commission's CCTV system, covering areas of the building located outside the OLAF security perimeter. This system is managed by the Directorate Security of the Commission's Directorate-General for Personnel and Administration ("**Directorate Security**" and "**DG ADMIN**") and has a different and broader scope than the OLAF CCTV system.

Of the two systems, only the system installed and to be operated by OLAF is covered by the Notification and comes within the scope of this prior checking Opinion. OLAF's CCTV

system had already been installed but it will only be put to use as from the date when the EDPS will have issued this Opinion and OLAF will have implemented the recommendations contained in the Opinion.

2.2. Location of the cameras and their field of vision. OLAF's CCTV system has 49 cameras. The cameras are all located inside OLAF's secure perimeter within the Commission building housing OLAF.

The field of coverage of OLAF's CCTV system, first, extends to the access and exit points to and from the OLAF secure premises [indication of precise locations omitted from the version of the Opinion available on the EDPS website]. The cameras monitor locations where one can enter or exit from the premises, for example, near the elevators and exits from the stairways, as well as near emergency exits and entry points from the roof of the building.

In addition, the system, to a certain extent, monitors sensitive areas where extra physical security is required, such as

- the OLAF Document Management Centre, which contains sensitive operational documents [indication of precise locations omitted],
- computer rooms [indication of precise locations omitted],
- the IT storage area [indication of precise locations omitted], and
- the IT technical rooms [indication of precise locations omitted] where end-user network connections to the EC corporate network or to the OLAF secure network are physically distributed and where regular interventions by OLAF and DIGIT personnel are needed.

In practice, this means that there are cameras on each floor occupied by OLAF. The computer rooms, the IT storage area and the IT technical rooms are normally unattended and contain very sensitive OLAF IT equipment as well as standard Commission corporate IT equipment. OLAF wants to be able to check what equipment was the object of any technical intervention in these rooms. This is especially important as intervention by external staff may occasionally be required on these premises.

None of the cameras monitor areas where staff would be continuously present and there are no instances where a staff member working in a certain area would be constantly in the field of vision of a camera.

There are also no cameras in individual offices, in the cafeteria/kitchen areas, near or in restrooms, or in other areas where staff members and visitors would expect a high degree of privacy.

Neither is the cameras' field of vision directed towards parts of the Commission building occupied by others than OLAF.

On the ground floor, there are OLAF cameras near the reception area; however, these cameras only focus on the elevators and stairways and only record the persons entering or leaving OLAF. A person has to have passed OLAF's automatic access control doors before being recorded by the system. Cameras are not installed in staircases, lifts, or lobbies on floors that do not provide an access to or from outside the OLAF secure perimeter.

The cameras in the parking lot are operated by the Commission's CCTV system.

Finally, the cameras' field of vision is also not directed to any areas outside the building on Belgian territory, with a view of neighbouring streets, buildings or other private or public areas.

2.3. Image quality. The resolution of the cameras is 1280 X 960 pixels. This allows OLAF to capture recognizable facial images.

2.4. Motion detection. All OLAF cameras come equipped with the functionality to use motion detection. This feature will be active on all cameras in order to trigger video recording. Motion detection will limit video signals to events worthy of observation and recording. This means that the cameras will record only when a movement is detected. Motion detection will always be used, twenty-four hours a day, seven days a week, both within and outside office hours. The camera automatically adds the motion information in the stream of data sent to the recording device. The recording device will only record if a camera informs it of detected movements.

2.5. Sound recording. When commenting on the draft EDPS Opinion, OLAF noted to the EDPS as a new element to the facts of the case that the cameras can record sound. Indeed, OLAF explained that the sound recording capability is required by the terms of reference of the call for tender for OLAF's "EUCI Registry Visitors" access control system. The sound recording feature, however, has not yet been implemented.

2.6. "High-end video-surveillance", cameras hidden from view or other intrusive features. OLAF does not plan to use other techniques or tools that may be described as "high-end video-surveillance". For example, it does not plan to use intelligent video-surveillance systems containing facial or other image recognition software, or gait recognition software. It also has not installed a network of multiple cameras, complete with tracking software that can track moving objects or people throughout the whole area. Neither has OLAF installed cameras that are hidden from view (e.g. rooftop cameras) or that are remotely controlled (point, tilt and zoom cameras). The cameras are also not equipped with thermal imaging devices for low light conditions (infrared and near-infrared cameras).

2.7. Sensitive data. OLAF does not plan to install any cameras at locations where there is an increased likelihood that sensitive data (as per Article 10(1) of Regulation (EC) No 45/2001) would be regularly captured on camera. These include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life. For example, OLAF does not have any cameras installed in an area outside its buildings where demonstrators would be potentially in the field of vision of cameras. Neither are there cameras at the entrances to a social worker's office, trade union's office or to a staff committee's office. There are no areas dedicated to the provision of medical services or for religious purposes within the OLAF secure premises.

2.8. Issues relating to the purpose of the processing and proportionality

2.8.1. Security risks in the areas covered by the OLAF CCTV system. OLAF does not have an internal document which would specifically list, define and evaluate what security risks the planned CCTV system is expected to reduce. However, OLAF confirmed that the types of security risks which the CCTV system is designed to address relate mainly to unauthorised physical access, and include the following:

- Unauthorised access to the OLAF secure premises and protected rooms;
- Unauthorized access to the OLAF secure IT infrastructure;

- Unauthorized access to OLAF's operational information;
- Theft of EC or staff-owned equipment or assets;
- Threats to the safety of OLAF's personnel working at the office.

2.8.2. History of security incidents at OLAF. The EDPS requested OLAF to provide statistics and examples on incidents that actually happened on OLAF premises in the past. More specifically, the EDPS requested statistics for the past five years and a copy of OLAF's register of security incidents.

OLAF answered to the EDPS that it does not currently have a register of security incidents. OLAF explained that the low number of detected incidents did not appear to require establishing a registry of incidents. However, it is noted that the low number of detected incidents (and the long detection time) may have been in part due to the absence of adequate incident detection capability in OLAF. OLAF confirmed that with the introduction of the new OLAF security systems a formal incident registry will be put in place and incidents will be regularly analysed to help improve and adjust the system as necessary.

As a register of security incidents and full statistics were not available, and considering also that OLAF has stated that it plans to monitor the system and its effectiveness more closely in the future, the EDPS accepted that OLAF only describes a few characteristic examples of past incidents and provides estimates of frequency of occurrence to illustrate the actual security needs of OLAF.

OLAF described to the EDPS three of the most significant security incidents that occurred over the past five years. All three cases involved unauthorized access to OLAF's secure premises, and potentially to OLAF's operational information, outside working hours by unidentified persons.

2.8.3. The role of the new CCTV system in assisting OLAF in deterring, preventing and investigating security incidents. OLAF explained to the EDPS that it is organising and implementing better and specific security measures since adoption of its Information Security policy, including both IT and physical security protections - which will provide OLAF with improved incident detection capabilities. The new CCTV system is part of this effort. It will be much quicker and easier to identify the persons at the origin of any similar security incidents that may occur in the future. OLAF security staff will be able to detect or confirm during an investigation whether unauthorised access to sensitive IT systems installed on the premises occurred and if so, by whom. It will also be able to prevent more efficiently unauthorized access during a security incident. The benefits of the new CCTV system will be mainly due to the following:

- Cameras will be installed at access points and other strategic locations (e.g. computer rooms). OLAF noted that three additional floors of the building [indication of precise locations omitted] were added to the OLAF secure premises after the cameras of the old Commission CCTV system were installed, and this resulted in additional access points to the OLAF secure premises [indication of precise locations omitted]. The new system will monitor those points, and will also cover the accesses from the roof of the building (a safety measure imposed by the fire department).

- Other strategic locations (e.g. computer rooms, as discussed above) will also be monitored.

- The footage can be used to investigate incidents which have already occurred.

- The new CCTV system can also prevent incidents by generating an alarm automatically reported to the OLAF Security Permanency, allowing immediate reaction by OLAF security personnel.

Additional technical features will bring added benefits. These include the following:

- The three physical control systems of OLAF will be integrated (see Section 2.8.4 below). For example, the system clocks of all three OLAF security systems are synchronised, so finding the right footage will be easier and quicker.

- Resolution of the new cameras is much higher than those of the old system, allowing clearer picture and easier identification.

- The cameras are oriented in such a way that meaningful video footage is obtained (e.g. also of the face and not only of the back of the person exiting through an emergency door).

2.8.4. CCTV as part of a broader set of physical security systems at OLAF. The CCTV system will be one of the three OLAF-specific physical security systems. The other two OLAF-specific physical security systems are

- an Access Control System, which regulates access to - and within - the OLAF secure premises and is the subject of another notification submitted to the EDPS for prior checking, and
- the physical Intrusion Detection System installed in certain very sensitive areas, e.g. computer rooms and the OLAF Document Management Centre.

In addition, the standard Commission security policies apply as minimum safeguards for protection of the OLAF building, staff safety, fire protection, and for safeguarding Commission information and other assets. DG ADMIN's Security Directorate is the provider of those safeguards.

OLAF emphasised that a high level of security can only be achieved by combining a variety of different security methods. The examples of past security incidents (see Section 2.8.2 above), in OLAF's view, demonstrate the security weaknesses of the current access control system.

OLAF believes, in particular, that the CCTV system will allow reconstructing what has actually occurred at key locations of the OLAF secure perimeter during a security incident, especially outside normal office hours. This was not always possible under the previous security arrangements in place.

2.9. Recording and live monitoring. The camera footage is recorded but it is not continuously or routinely monitored live, for example, by security guards in a control room or at the building reception.

Any camera footage will only be viewed if there is a security incident and there is a need to view the camera footage either

- to help investigate what happened (that is, the videos are recorded for à-posteriori analysis)

- or if there is a need for immediate intervention. As discussed above, there is an automated alert system to call the attention of OLAF security staff of any incidents. OLAF security staff (the local security officer, the deputy security officer and the network operation security officers) will be able to instantly access OLAF's live videos should the need arise.

2.10. Conservation period. Recorded data will be kept for no longer than one year. This means that all CCTV footage of all 49 cameras may be kept for an entire year even if (i) there has been no security incident detected during that year at all, or if (ii) only the footage of certain cameras is relevant for investigating the security accidents that actually happened. Videos are stored online for five months, then off-loaded and stored off-line for a maximum of seven months before being destroyed. Thus, twelve months is the total maximum retention period of any video footage.

If, however, a particular footage is relevant to the investigation of a security incident, it will be exported and placed in the relevant incident investigation file, until the end of the investigation or of its eventual disciplinary or judicial follow-up. Thereafter, it will be destroyed.

No data are stored for historical, statistical or scientific purposes.

In OLAF's view the specified retention period is necessary because not all security incidents are discovered immediately. For example, some security investigations were triggered only two or three years after the leak of a sensitive OLAF operational document. OLAF further argued that a one year total retention period is reasonable in the case of OLAF, given the sensitive nature of its operational business.

OLAF provided no further data as to (i) how often a security incident was discovered with such a long delay and (ii) why other technical and organizational security measures cannot be taken to ensure that security incidents recorded by the CCTV system (mainly unauthorized physical access) are detected earlier, and thus, can trigger an earlier investigation.

2.11. Recipients

2.11.1 OLAF security staff. The CCTV system is used and operated by OLAF's in-house security staff, which consists of:

- the local security officer[1],
- the deputy security officer, and
- three statutory staff members responsible for daily operations of OLAF's specific security systems.

The head of OLAF's Information Services Unit, of which the security sector is a part, does not have direct access to the footage of the cameras (no password and no individual monitor in his office). However, he will be provided indirect access by any of the five OLAF security staff members if the need arises such as when a decision needs to be made whether certain CCTV footage can be transferred to third parties. In this case and in other cases where data protection issues need to be considered access may also be provided to OLAF's DPO.

Data protection training is foreseen for all OLAF staff during the course of 2008.

[1] The local security officer (LSO/LISO) is Head of the Sector "Network Operations and Security" (NOS).

2.11.2. Outsourced security staff (and security guards in general) will have no access to the CCTV footage. The CCTV system was initially installed by the private company which provided the system. OLAF has a technical maintenance contract with this company. However, none of the daily CCTV operations have been outsourced. No security guards (whether in-house or outsourced) will have access to OLAF's CCTV system.

In case of a technical failure requiring intervention by technical experts from the system provider, access to live or stored videos by such personnel will be limited to the strict minimum required for testing and demonstrating that the system is again fully operational at the end of the intervention. The contractor has signed a general non-disclosure agreement for the overall system and is bound by this even after the contract has ended. Each technician working on the system will have to sign a non-disclosure agreement as well.

2.11.3. Accessing CCTV footage; log files and registers. Each of the five OLAF security staff members will have direct access to and will be able to monitor the footage of any cameras live at any time. Three monitors will be installed: one in the office of the local security officer, another one in the office of the deputy local security officer and one in the office of the network operations security officers.

These systems are password-protected. OLAF security staff log on and off only as needed. They log off whenever they leave their offices unattended. In addition, the doors are locked and the door will be equipped with an intrusion detection system. Each OLAF security staff member is technically able to delete or copy any CCTV footage. However, they cannot alter the footage, except when exporting it to a DVD as specified in section 2.13 below.

If a security incident is detected or suspected, it is each OLAF security staff member individually who may decide whether there is a need to access (live or recorded) CCTV footage. The decision is documented in a report of any suspected or confirmed incident to the local security officer.

There are log-files about who accesses, views, copies, alters or deletes the CCTV footage. The system's logs are exported in near-real time to the Core Business Information System's Security Information and Events Management System (CBIS SIEMS in short), which logs all OLAF security events. The CBIS SIEMS does not allow alterations of its logs. The system is operated by the network operation security staff members.

Beyond log-files, there is no electronic or paper-based register documenting access to CCTV footage. However, as noted above, access is documented in the reports about suspected or confirmed incidents submitted to the local security officer.

2.12. Data transfers

2.12.1. General policy on transfers. OLAF does not have a formal written policy on who else may be granted access to CCTV footage beyond the OLAF security staff members, as described above.

However, OLAF explained to the EDPS that any request would be handled by the controller, that is, the head of OLAF's Information Services Unit, following consultation with OLAF's DPO. It would be documented by a note to the file.

Further, any request for access to CCTV footage would be handled in accordance with

- Articles 7, 8 or 9 of Regulation (EC) No 45/2001,

- Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents, and

- Articles 8 to 10 of Regulation (EC) No 1073/1999 concerning investigations conducted by OLAF.

A determination of whether to grant access will be made on a case-by-case basis. In any event, no systematic or routine transfers are foreseen.

2.12.2. Transfers within OLAF. The EDPS requested OLAF to specify in what cases persons within OLAF other than OLAF security staff or the data subjects (e.g. management or human resources) will be given access. OLAF emphasised that the determination will be made on a case-by-case basis as explained in Section 2.12.1 above.

2.12.3. Transfers to the Security Directorate of the Commission. OLAF has not interconnected and does not plan to interconnect OLAF's CCTV system with the CCTV system operated by DG ADMIN's Security Directorate.

Indeed, no access is given to the Security Directorate of the Commission directly or in the absence of a specific incident. The Security Directorate does not have direct access to the CCTV footage. The decision whether to give access to CCTV footage to the Security Directorate of the Commission if a security incident is detected or suspected will be made on a case-by-case basis as explained in Section 2.12.1 above.

2.12.4. Transfers to the Commission's Investigation and Disciplinary Office ("IDOC"). OLAF may transfer the relevant footage (for example, footage that may serve as evidence) in case such footage is requested by 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. The determination will be made on a case-by-case basis as explained in Section 2.12.1 above.

2.12.5. Transfers outside the EU institutions. The EDPS also requested OLAF to explain in which cases and subject to what procedure third parties outside the EU institutions (e.g. Belgian police, courts or the media) will be given access to CCTV footage.

More specifically, the EDPS requested whether OLAF requires a written request signed by a police officer or a court order issued by a judge, similar to the warrant to search someone's home. The EDPS also requested whether (i) OLAF requires that the request specify the reason why the CCTV footage is needed, (ii) whether the request has to relate to a specific investigation, and (iii) whether there are any further conditions that the request must fulfil.

The EDPS also specifically requested whether courts in civil, commercial, administrative, or labour law matters are allowed to have access to CCTV footage. Additionally, the EDPS also asked whether (i) defendants or their lawyers are allowed to have access to CCTV footage if they are charged or if they expect to be charged with a criminal offence and (ii) whether parties (or their lawyers) in a civil, commercial, administrative, or labour law dispute are allowed access to CCTV footage.

In its response OLAF indicated that any such requests must be handled on a case-by-case basis. For matters where Community interests are at stake, OLAF would be guided by the ruling of the decision of the European Court of Justice in *Zwartveld et al*[2] to the effect that a request by a Member State court for access to information is governed by the principle of loyal cooperation which imposes mutual duties in this regard. If no Community interest were at stake, Belgian law would govern.

OLAF also confirmed that if a Member State police or other national organization requested access in the course of an official proceeding (and thus not within the framework of Regulation (EC) No 1049/2001 or Regulation (EC) No 45/2001) it would first be obliged to obtain a waiver of immunity if the footage concerned an EU staff member.

Finally, OLAF also confirmed that it believes it has no legal basis to grant access to private parties other than Regulation (EC) No 1049/2001 or Articles 7-9 and 13 of Regulation (EC) No 45/2001), and therefore, it expects that accommodation of any such access requests would occur only under very rare and specific circumstances. Any such requests will be evaluated on a case-by-case basis as explained in Section 2.12.1 above.

2.12.6. Manner of transfer. No direct access will be provided to anyone other than OLAF's security staff. Instead, OLAF's security staff will show authorised recipients the CCTV footages relevant to the case. OLAF's security staff may also provide any copy of CCTV footage relevant to the case on a DVD.

2.13. Access rights of data subjects. If a data subject requests access to his/her data, OLAF plans to provide a copy of the footage on a DVD or make an appointment for viewing the CCTV image. The procedure for addressing access requests will be as follows:

- The data subject can ask for access to his/her recorded image at a specified time and location. OLAF will reply within 15 working days.
- An OLAF security staff member will view the footage to determine whether the data subject is in it.
- An appointment will be made with the data subject to view the video. If the data subject requests a copy of the footage where his/her image appears, OLAF will provide it on a DVD, unless one of the exemptions specified in Article 20 of Regulation (EC) No 45/2001 is applicable.

For footages that are exported on a DVD, third parties not relevant to the specific request will be anonymized by a member of the network operation security staff through video editing of the mpeg2 export. However, as it may not always be feasible to do this, consent of other data subjects present on the same footage may be required in such case. In case of doubt, the head of OLAF's Information Services Unit will decide whether the footage can be provided, in consultation with the DPO.

OLAF's present policy is not to charge for producing the copy of the footage.

2.14. Notice to data subjects. OLAF plans to provide detailed information to data subjects in several different forms. In particular, it will

- post a privacy statement on its intranet and internet sites,
- make available leaflets at the building reception providing the same text, and

[2] Case 2/88, ECR 1990, I-3365.

- provide a more limited notice on the spot as well.

2.14.1. Signs on the spot. As for the on-the-spot notice, signs of A3 size indicating video surveillance are already posted at the main entrance. These relate to the old CCTV system. OLAF plans to put the ISO pictogram for video surveillance on all entry points of the OLAF security perimeter in addition to the signs at the main entrance.

The information on the signs (next to each pictogram) will include the following:

- the name of the controller (OLAF),
- the purpose of processing,
- the fact that recording takes place, and
- contact information (website address).

2.14.2. More detailed privacy statement for the CCTV system. OLAF provided a copy of its draft privacy statement to the EDPS. The two-page document includes the following information:

- brief description of the coverage of the CCTV system (entry and exit points, computer rooms, etc),
- what personal information the CCTV system collects, for what purpose and through which technical means,
- who has access to the CCTV footage,
- how OLAF safeguards the information,
- how long OLAF keeps the data,
- how can data subjects verify, modify or delete their information, and finally,
- the notice also points out to the right of recourse to the EDPS.

2.14.3. Regular information to staff about ongoing security plans. Finally, OLAF explained to the EDPS that its staff has been regularly informed of the ongoing security plan since the adoption of the OLAF Information Security Policy. This has occurred through (i) publication on the OLAF Intranet of decisions taken by the various competent committees, (ii) ad-hoc security presentations to user groups, and (iii) monthly security introductions to newcomers. In addition, an e-mail was sent to all staff on 1 February 2007 before the three new physical control systems were installed, explaining to them the work in progress on the new system.

2.15. Security measures.

[...]

3. Legal analysis

3.1. Prior checking

3.1.1. Scope of Notification. As noted in Section 2.1 of this Opinion, the scope of the Notification and of this Opinion covers the data protection aspects of OLAF's newly installed CCTV system but does not extend to the Commission's CCTV system, which also operates in the Commission building which houses OLAF.

3.1.2. Applicability of the Regulation. Pursuant to its Article 3, Regulation (EC) No 45/2001 applies to the

- processing of personal data
- wholly or partly by automatic means (or to the processing of personal data which form part of a filing system), provided that
- the processing is carried out by Community institutions and bodies
- in the exercise of activities which fall within the scope of Community law.

All elements that trigger the application of Regulation (EC) No 45/2001 are present here:

First, operation of the CCTV system entails the collection and processing of personal data as defined under Article 2(a) of the Regulation. Second, the personal data collected undergo "automatic processing" operations as well as manual data processing operations, and the data form part of a filing system (Article 3(2) of the Regulation). Indeed, personal data such as the images of staff members and visitors are automatically recorded, and in some cases, also monitored live. They are subsequently stored on-line and off-line and remain searchable by time and location. Some images may also be retrieved, viewed, copied, altered, and transferred to other recipients.

Third, the processing is carried out by OLAF, a Community body, and in the framework of Community law (Article 3(1) of the Regulation).

Based on the foregoing, Regulation (EC) No 45/2001 is applicable.

3.1.3. Grounds for prior checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS all "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". Article 27(2) contains a list of processing operations that are likely to present such risks.

As this was his first prior checking case dealing with CCTV systems, the EDPS had to analyse whether such systems in general, and the CCTV system operated by OLAF in particular, present such specific risks, and therefore, should be subject to prior checking.

During this analysis, the EDPS considered that video-surveillance, by its nature, is an invasive technology and one that is easily abused. In addition, wide-spread video-surveillance also has significant social costs. On the other hand, the EDPS also acknowledged that not all CCTV systems present the same level of risks to privacy.

The EDPS first points out that video-surveillance, even if the CCTV footage is not recorded, is significantly different from surveillance by security personnel on the spot. Unlike one or more uniformed persons openly observing their targets with a naked eye, in case of video-surveillance the person observed does not know who observes him and for what reason. If the cameras are not positioned in plain view or if there is not an appropriate notice provided on the spot, he may not even be aware that he is being monitored.

As a technical matter, surveillance cameras can zoom in on a subject, record images, match images against a database of images, or track moving objects in large areas. If the recordings are conserved for a long period of time, there is an increased risk of “mission creep”, that is, an increased risk that the images may be used for purposes not contemplated and specified initially.

Further, digital images are also easily copied and distributed. They can, indeed, be broadcast to a multitude of recipients or posted on the internet. Even if the images are not recorded by

the operator of the CCTV system, and only transferred to the intended recipients via an internal network, the images may be intercepted by hackers en route, or recorded and subsequently used for incompatible purposes by one of the recipients.

These features of video-surveillance offer very real opportunities for security breaches and misuse: the footage may fall into the wrong hands or may be used by the lawful recipients for unlawful purposes.

The risks of video-surveillance, however, go beyond the instances when actual abuse happens. Indeed, knowing that our every move and gesture is monitored by the cameras may, in case of widespread or continuous surveillance, put us under significant psychological stress as we need to constantly adjust our behaviour to the expectations of those who are operating the surveillance cameras. This constitutes a significant intrusion into our privacy, which must be balanced against the benefits achieved from the use of CCTV.

Still further, video-surveillance also has its social costs. It may not only deter criminal activities but also all other forms of non-conformist behaviour.

Due to these considerations, the EDPS concludes that CCTV systems are likely to present specific risks to the rights and freedoms of data subjects, in the meaning of Article 27(1).

With that said, the EDPS also emphasises that CCTV systems come in all shapes and sizes and range from the small and simplistic to the large, complex and highly sophisticated, and from the barely noticeable to the highly intrusive. Therefore, a case by case analysis is necessary to decide whether a specific CCTV system needs to be submitted for prior checking under Article 27(1).

As regards the CCTV system proposed by OLAF, in the absence of the availability of the final version of the video-surveillance guidelines, the EDPS decided to prior check the system to assist OLAF in achieving full compliance. In addition, on one key issue, the length of the conservation period, OLAF's plans described in the Notification significantly differed from those that will be recommended by the EDPS in his guidelines. This also confirms that prior checking of OLAF's plans can add value and help ensure more complete compliance with data protection requirements.

3.1.4. Notification and due date for the EDPS Opinion. The Notification was received on 17 October 2007. According to Article 27(4) of Regulation (EC) No 45/2001 this Opinion must be delivered within a period of two months. The procedure was suspended for a total of 153 days. Thus, the Opinion must be rendered no later than 19 May 2008 (18 December 2007 + suspensions for 110 days + 14 days + 29 days for comments).

3.1.5. True prior checking. The processing operations were notified to the EDPS after the installation of the CCTV system but before the controller started to operate the system. The EDPS issued his Opinion on 19 May 2008.

Since prior checking is designed to address situations that are likely to present risks, the opinion of the EDPS should normally be requested and given prior to the start of the processing operation. The EDPS welcomes that he had been consulted before OLAF started to operate its new CCTV system and that the DPO of OLAF had been involved in the decision-making regarding OLAF's CCTV system from an early stage.

In this case, as it will be shown in Section 3.2 and 3.4 below discussing lawfulness and proportionality, the EDPS concluded that the purposes of OLAF's CCTV system are lawful and the size and set-up of the CCTV system (hardware, software and human resources) is proportionate. Therefore, any recommendations made by the EDPS to improve privacy compliance can be achieved without dismantling or relocating any CCTV cameras or making other costly adjustment to the system. As this may not be the case with every CCTV system notified, the EDPS encourages early notifications (before installation and investment in the system) and/or close involvement of the DPO in the decision-making right from the beginning.

3.2. Lawfulness of the processing. Article 5(a) of Regulation (EC) No 45/2001 provides that personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties ... or other legal instrument adopted on the basis thereof".

The first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing: a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is necessary for the performance of a task carried out in the public interest. To address this second issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies". Thus, the second issue in the present case is whether the processing is necessary and proportionate for the management and functioning of OLAF.

Legal basis. With regard to the first issue, the Notification lists a number of documents as the legal basis of the CCTV operations as follows:

- Article 297 of the EC Treaty;
- Article 17 of the Staff Regulations;
- Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office: Recitals 4, 17, 18; Articles 8, 11(1), and 12(3);
- Commission Decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF): Recitals 4, 5; Articles 2 (5) and 3;
- Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending the Commission's Internal Rules of Procedure: security provisions;
- Commission Decision C(2006) 3602 of 16 August 2006 on the security of information systems (available at http://intracomm.cec.eu-admin.net/security/legislation/legislation_en.htm);
- the Commission's Information Systems Security Policy (currently under review, obsolete, non-official version of 2001 available at http://intracomm.cec.eu-admin.net/security/legislation/legislation_en.htm); and
- OLAF's Information Security Policy (Section 4.5 of the OLAF Manual[3])

Of these, the first four documents are only indirectly relevant to OLAF's CCTV system. In contrast, the second set of four documents listed by OLAF are directly relevant to the security measures that OLAF may be taking in order to secure unauthorized physical access to its

[3] The latest version of the OLAF Manual is that of 25 February 2005. A new manual is under preparation.

premises, IT infrastructure, and operational information, which is the purpose of OLAF's CCTV operations.

Nevertheless, none of these documents specifically require the installation of a CCTV system in the framework of ensuring the safety and security of OLAF's operations. Indeed, the referred documents only very infrequently mention CCTV at all.[4] Upon request by the EDPS, OLAF confirmed that it has not adopted itself any documents specifically discussing CCTV at OLAF either. To OLAF's knowledge, the Commission or its Directorate Security also have not adopted any documents specifically discussing CCTV.

Thus, specific legal instruments adopted on the basis of the Treaties do not provide the detailed conditions for the operation of OLAF's CCTV system. Nevertheless, the EDPS considers that the more general documents listed provide sufficient legal basis for the installation and operation of OLAF's CCTV system.

With that said, the EDPS would find it desirable if OLAF adopted internal guidelines which would

- describe the purposes, set-up and use of its CCTV system and
- provide for the data protection safeguards already in place or recommended in this Opinion.

Proportionality. With regard to the second issue to be analysed when examining the lawfulness of OLAF's CCTV system, the EDPS is also satisfied and does not challenge that the notified processing operation is necessary and proportionate for the management and functioning of OLAF. The EDPS based his conclusions on proportionality primarily on the following facts:

- The purposes of the system are clearly delineated, relatively limited, and legitimate: the main purpose of OLAF's CCTV system is protection against unauthorized physical access, in particular, to sensitive operational information and IT equipment.
- The location, field of coverage and resolution, and other aspects of the set-up of the CCTV system appear to be adequate, relevant and not excessive in relation to achieving the specified purposes, taking into consideration also the sensitivity of the information held by OLAF: in particular, cameras are only located near exit and entry points to the OLAF secure area and at certain other strategic locations such as certain unattended IT rooms and the OLAF Document Management Centre.

[4] OLAF explained that Section 18.3.8 of Commission Decision 2001/884/EC specifies that "when alarm systems, closed circuit television and other electrical devices are used to protect EU classified information, an emergency electrical supply shall be available to ensure the continuous operation of the system if the main power supply is interrupted. Another basic requirement is that a malfunction in or tampering with such systems shall result in an alarm or other reliable warning to the surveillance personnel." OLAF confirmed that both requirements are met with OLAF's CCTV system. All parts of the CCTV system are protected by an Uninterruptible Power Supplies (UPS) system and the central Security Information and Events Management System (SIEMS) collects alarms from all systems.

This is with the caveat that certain aspects of the processing that go beyond what is proportionate will need to be modified. This applies, in particular, to the conservation period, as will be discussed in Section 3.5 below.

In addition, the EDPS also calls OLAF's attention to the fact that before OLAF activates the sound recording feature on any of its cameras in the framework of its new access control system, it should (i) establish strict data protection safeguards and (ii) request the prior opinion of the EDPS. Till then, the sound recording facility should be turned off or disabled in some other way. In any event, the EDPS points out that CCTV must not be used to listen to or record conversations between members of the public as this is highly intrusive and unlikely to be justified.

To conclude, the EDPS considers that the notified processing operations are lawful, so long as the recommendations made in this Opinion are followed.

3.3. Processing of special categories of data. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited unless an exception can be found in Articles 10(2)-(4) of Regulation (EC) No 45/2001.

The EDPS, first, emphasises that CCTV footages inherently reveal some indication about the ethnic or racial origin of the persons caught on the cameras. This is unavoidable, and without the existence of further risk factors, does not mean that the processing should be prohibited as one that would come within the meaning of Article 10 of the Regulation.

In the present case,

- There is no intention on the part of OLAF to collect and process any sensitive data;
- Sensitive data would be caught on cameras only very infrequently and purely incidentally. In particular, there are no medical, religious, or trade union establishments within the areas covered by the CCTV system, and it is also unlikely that any demonstrators would come within the field of vision of the cameras.
- The security of the internal CCTV system, the data protection safeguards taken, and the limited number of recipients (five security staff) suggest that the risks that any sensitive data would fall into the wrong hands or would otherwise be misused are relatively limited.

Therefore, the EDPS concludes that Article 10 does not prohibit OLAF from installing and operating its CCTV system according to its plans as described in this Opinion. With that said, the EDPS recommends that the data protection training provided to OLAF security staff specifically call the staff’s attention to the fact that the data they are handling, in some cases, may qualify as sensitive data, and therefore, they should be particularly careful in safeguarding them. The training should also explain that during investigation of security incidents, they should not profile those caught on the cameras based on them belonging to a particular race, religion, or ethnic background.

3.4. Data Quality

Adequacy, relevance, and proportionality. According to Article 4(1)(c) of Regulation (EC) No 45/2001 personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."

Apart from the issues related to the length of the conservation period, which will be discussed in Section 3.5, based on the information provided to him, the EDPS does not challenge the adequacy, relevance and proportionality of the installation and operation of OLAF's CCTV system. With that said, the EDPS emphasizes that compliance with these three principles always requires an analysis "in concreto", on a case by case basis.

Fairness and lawfulness. Article 4(1)(a) of Regulation (EC) No 45/2001 requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 3.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 3.8 below).

Accuracy. According to Article (4)(1)(d) of the Regulation, personal data must be "accurate and, where necessary, kept up to date", and "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."

Based on the information provided to him, the EDPS does not challenge the accuracy of the video data collected by OLAF's CCTV system. In particular, OLAF confirmed that its cameras have sufficient resolution to provide recognizable facial images. In addition, OLAF also confirmed that the cameras are positioned and located in such a way as to obtain meaningful images to help identify the persons at the origin of the security incident. Time and location are also indicated on the footage.

3.5. Conservation of data

The general principle of Regulation (EC) No 45/2001 is that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article (4)(1)(e) of the Regulation).

The EDPS is of the opinion that the arguments raised by OLAF during this prior checking procedure to justify the proportionality of a one-year conservation period are insufficient. On the facts of the case, the EDPS found that the one-year conservation period designated by OLAF is excessive.

The type of security incidents mentioned by OLAF to the EDPS as illustrations of its security needs and justifications of the need for the CCTV system all included unauthorized physical access to OLAF premises and potentially to sensitive OLAF operational information.

These security incidents would or should typically be detected either immediately, by way of an alert, or at most, in a matter of days. For example, a door to a secure premise which was accidentally left open at the end of the day would or should, at the latest, be discovered the next morning. OLAF's two other physical access control systems should be, and as far as the EDPS is aware, indeed are, regularly monitored and any intrusion or system failure should be detected nearly instantaneously.

If this is not the case, instead of disproportionately extending the conservation period for CCTV footage for the eventuality that the occurrence of a security incident might come to

light after several months or years, OLAF should be working on improving its security incident detection and prevention capabilities.

The theoretical possibility that a leak of an operational document might only come to light several years after the date when the document may have been unlawfully accessed, and in such cases, a-posteriori review of several years of CCTV footage might help investigate who might have leaked the document is not sufficient to justify the proportionality of keeping all CCTV footage for a year or more.

The EDPS also points out that the international practice among those European countries whose legislation or national data protection authorities do provide a maximum permissible conservation period, provide no more than one month as an upper limit for conservation of CCTV footage. As a matter of fact, CCTV footage used for security purposes is commonly erased and overwritten within a matter of days, which is usually sufficient to detect any unauthorized access, theft, or other criminal activity that may be caught on the cameras.

Based on the foregoing, the EDPS recommends that OLAF reassesses the necessity of keeping all CCTV footage for a period of one year. During this assessment it must bear in mind that conservation periods should closely match the periods during which access to the personal data may be necessary for clearly specified purposes. OLAF should, in particular, assess how long it needs to keep the data to reveal that unauthorised physical access has indeed happened. The EDPS recommends that the CCTV footage should be erased in a matter of days or weeks, the exact conservation period to be decided based on OLAF's internal assessment of its needs.

3.6. Recipients and data transfers

The EDPS welcomes the fact that the scope of the foreseen recipients is limited to OLAF's five security staff, in the manner described in Section 2.11.3 above.

Considering that appropriate system logs are made (as described in Section 2.11.3 above), the EDPS finds it acceptable that all five members of the OLAF security staff are able to view and copy CCTV footage. However, the EDPS recommends that OLAF reconsiders whether it is not sufficient if only a more limited number of persons within OLAF's security team are given the technical possibility to alter and delete CCTV footage. For example, the possibility to make these interventions could be limited to the local security officer and the deputy security officer.

The EDPS also considers that ad hoc data transfers to DG ADMIN's Directorate Security and to IDOC, subject to the safeguards described by OLAF in Section 2.12 above, are in compliance with Article 7(1) of Regulation (EC) No 45/2001, which provides that personal data may be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient. The EDPS emphasizes that pursuant to Article 7(3), the recipients shall process the personal data they received from OLAF only for the purposes for which they were transmitted.

The EDPS also welcomes OLAF's commitment that if unforeseen data transfers are requested by any third party (within or outside OLAF), OLAF should allow transfers only as specifically allowed by Regulation (EC) No 45/2001. The EDPS especially welcomes OLAF's practice that in case of doubt, the head of OLAF's Information Services Unit consults OLAF's DPO before he makes the requested data transfer.

3.7. Right of access and rectification

Right of access. According to Article 13(c) of Regulation (EC) No 45/2001, the data subjects have the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing the processing and any available information as to their source. Article 20 provides for certain restrictions to this right including the case when such a restriction constitutes a necessary measure to safeguard the protection of the data subject or of the rights and freedoms of others.

The EDPS welcomes that OLAF confirmed that it provides access to the CCTV footage to data subjects should they so request. The EDPS also welcomes that OLAF established safeguards to ensure that

- any access requests will be dealt with in a timely fashion (within fifteen days) and
- without constraints (access requests do not need to specify the reason for the request) and that
- the rights of third parties are safeguarded by image-editing or requesting consent.

The EDPS also welcomes that the head of OLAF's Information Services Unit consults the OLAF DPO should he wish to limit access to any data requested.

Right of rectification. Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Due to the nature of CCTV footage, there is relatively little likelihood that data subjects would need to rectify their data, although it is always possible that the time or location of the CCTV footage may be erroneously indicated, or that the report written by security staff in connection with a security incident erroneously identify the data subject or contain other errors. The EDPS recommends that OLAF establish similar safeguards to those it applies to the right of access to ensure that data subjects can confidently exercise their rights of rectification, should the need arise.

3.8. Information to the data subject

Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. Article 11 is applicable to data obtained from the data subject, whereas Article 12 is applicable to cases where the data have not been obtained from the data subject. Thus, it is Article 12 which applies to the CCTV footage.

Timing and format of the data protection notice. Article 12 provides that the information must be given when the data are first recorded or disclosed, unless the data subject already has it.

The EDPS, in his video-surveillance guidelines, will recommend the combination of the following three methods for the provision of notice:

- notices on the walls of the buildings or fences to alert passers-by to the fact that monitoring takes place and provide them with the most important information about the processing,
- a detailed privacy policy posted on the internet for those who wish to know more about the video-surveillance practices, and

- hard-copy of the same privacy policy made available at the building reception upon request.

The availability of more detailed information on the internet and at the reception must not altogether substitute the notices placed outside the buildings. Rather, they should serve as a complement to them. The notices outside the buildings must include as much of the information listed under Article 12 as is reasonable under the circumstances. In any event, they must at least identity the controller and the purpose of the surveillance. They must also clearly mention that the images are not only viewed but are also recorded, provide contact information and mention the availability of further information on the internet and at the building reception.

Members of the security staff and reception should be trained about the privacy aspects of video-surveillance practices and should be able to make copies of the detailed privacy policies instantly available upon request. They should also be able to tell data subjects whom to contact if they have additional questions or would like to request access to their data.

The signs must be placed at such locations and in such size that data subjects can see and read them before entering the monitored zone.

The EDPS welcomes OLAF's good practice of providing the required data protection notice on-line, both on OLAF's external and internal websites. This reassures data subjects (OLAF staff as well as outside visitors) that their data will be processed fairly and lawfully. The EDPS also welcomes OLAF's practice of providing the same information, upon request, at the building reception. Finally, the EDPS welcomes that the number of currently available on-the-spot notice boards will be increased and their content will be revised and expanded.

Indeed, OLAF appears to closely follow the recommendations that will be incorporated into the video-surveillance guidelines. To ensure complete compliance, the EDPS calls OLAF's attention to the fact that the data protection training that OLAF foresees for its entire staff during the year 2008 should include the specific training of receptionists and security guards as described above.

Content of the data protection notice. Article 12 of Regulation (EC) No 45/2001 provides a detailed list of information that needs to be provided to data subjects. In essence, the controller must inform data subjects about who processes what data and for what purposes. The information must also specify the origins and recipients of data, must specify whether replies are obligatory or voluntary and must alert the data subjects to the existence of the right of access and rectification. Further information, including the legal basis of processing, the time limits for storing the data, and the right of recourse to the EDPS must also be provided if necessary to guarantee fair processing. This may depend on the circumstances of the case.

Finally, Article 12 allows certain exceptions from the notification requirement. Considering that (i) none of the Article 12 exceptions apply to the facts of the case, and that (ii) all items listed in Article 12 (including the legal basis of processing, time-limits for storing the data, and the right of recourse to the EDPS) are necessary to guarantee fair processing, the EDPS is of the opinion that all items listed under Article 12 must be provided in the data protection notice. This is with the exception of "the origins of data" and specification of "whether replies are obligatory or voluntary", both of which are self-explanatory on the facts of the case.

The EDPS welcomes that the data protection notice includes a brief mention of all but one items required in Article 12 of the Regulation. The EDPS recommends that the missing item

(legal basis) will be included in the privacy statement, once OLAF will have adopted the internal document recommended in Section 3.2 above.

The EDPS points out that it especially welcomes that the text of the data protection notice is written in a clear, concise, user-friendly manner, avoiding unnecessary data protection jargon.

Additional recommendations. The EDPS discusses below only those items listed under Article 12 where he suggests further changes.

Information about access rights. The EDPS recommends that information should go beyond merely mentioning the existence of this right and providing contact information, and should also discuss

- the timelines set forth in this Opinion (fifteen days),
- the manner in which OLAF will provide access (viewing or copying on a DVD),
- the manner in which it will safeguard rights of third parties (editing or consent), and
- the fact that OLAF does not plan to charge a fee for access.

Recipients. The information provided by OLAF during the prior checking procedure suggests that security guards have no access at all to CCTV footage. The privacy notice should be adjusted accordingly.

Reference to the EDPS Opinion. The EDPS further recommends that the privacy notice provides a reference and a link to this Opinion on the website of the EDPS.

3.9. Security measures. According to Article 22 of the Regulation, the controller must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

The EDPS notes that OLAF's specific IT infrastructure has been horizontally reviewed by the EDPS in a separate procedure. This prior checking Opinion is not the place to repeat that review. With that said, the EDPS has assessed the additional information that OLAF provided specifically in respect of its CCTV system. During his review, the EDPS has not encountered any facts which would suggest doubts about the adequacy of the security measures OLAF took in the framework of safeguarding the security of its CCTV footage.

Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001 provided that the considerations noted in Sections 3.2 through 3.9 are fully taken into account. The recommendations of the EDPS include, most importantly, the following:

- Legal basis:
  - OLAF should adopt an internal document describing its CCTV system and providing for appropriate data protection safeguards.

- Conservation of the data:

- OLAF should reconsider the planned conservation period to ensure that data are kept no longer than necessary for the purposes initially contemplated.

- Information to data subjects:
  - More specific and accurate information needs to be provided to data subjects regarding some items listed under Article 12 of the Regulation.

In addition, the EDPS emphasises that before OLAF activates the sound recording feature on any of its cameras in the framework of its new access control system, it should (i) establish strict data protection safeguards and (ii) request the prior opinion of the EDPS. Till then, the sound recording facility should be turned off or disabled in some other way. In any event, CCTV must not be used to listen to or record conversations between members of the public as this is highly intrusive and unlikely to be justified.

Done at Brussels, on 19 May 2008

(signed)

Peter HUSTINX
European Data Protection Supervisor