GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Johan Van Damme
Data Protection Officer
European Court of Auditors
12, Rue Alcide De Gasperi
1615- Luxembourg
LUXEMBOURG

Brussels, 20 December 2011
GB/UK/mch/ D(2011) 2328 **C 2011-0989**

Subject: Prior-checking notification case 2011-989 on the video-surveillance system at the European Court of Auditors (ECA)

Dear Mr Van Damme,

We reviewed the documents you have provided the European Data Protection Supervisor (EDPS) with on 28 October 2011 and, additionally, 7 November 2011 concerning the notification for prior checking under Article 27 of Regulation (EC) No 45/2001 (the Regulation) on the processing operations related to the video-surveillance system at the European Court of Auditors (ECA).

The EDPS issued Video-Surveillance Guidelines[1] (henceforth: "Guidelines") in March 2010, requesting the EU bodies and institutions to bring their existing practices in compliance with these Guidelines until 1 January 2011. In the present case, in the light of the notification of 28 October 2011, the EDPS will highlight only those ECA practices which do not seem to be in conformity with the principles of the Regulation and with the Guidelines and will restrict his legal analysis to those practices. It is clear that all relevant recommendations made in the Guidelines apply to the processing operations put in place in the frame of the video-surveillance system at the European Court of Auditors (ECA).

1. Need for prior checking

Section 4.3 of the Guidelines outlines the situations in which the EDPS considers that a prior checking notification under Article 27 of the Regulation is required to assist the relevant institution in establishing additional data protection safeguards in cases where its activities go

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf .

beyond the standard operations for which the Guidelines already provide sufficient safeguards. The situations referred to in Section 4.3 of the Guidelines include inter alia:

- video-surveillance proposed for investigative purposes;
- employee monitoring and processing of special categories of data;
- monitoring areas under heightened expectations of privacy.

a) *Video-surveillance proposed for investigative purposes*

The notification submitted (section 16 of the notification form) seems to suggest that the processing requires prior notification under Article 27(2)(a) ("*...processing of data relating to health and to suspected offences, offences, criminal convictions or security measures...*") and the Video-surveillance audit report notes (section 20) that "*The EDPS was notified with a view to a prior check in 2011, since images may eventually be used during an investigation".*

The ECA video-surveillance policy in its section 6.2 notes that "*The ECA uses its video-surveillance system for the sole purposes of security and access control...*"; its section 6.3 explicitly highlights that "*The system is not used for any other purpose"* and stipulates that *"Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access). Only in exceptional circumstances may images be transferred to investigatory bodies in connection with formal disciplinary or criminal investigations*". These exceptional circumstances are defined (in Section 7.4 of the ECA video-surveillance policy) as follows: "*Local police may be given access if needed to investigate or prosecute criminal offences...*". According to the Privacy Impact Assessment (section 5.1), "*If a criminal act has taken place and the proof of the act(s) is on the film or one could identify the authors of such acts, the recorded images could be handed over to national policy authorities*", which -as outlined in section 5.4 of the Privacy Impact Assessment- requires an official request from a *procureur*.

As noted in Section 5.8 of the Guidelines, it cannot be excluded that -in exceptional circumstances- video-surveillance might be used for investigative purposes, even when this is not directly triggered by a physical security incident. To decide whether these uses are permissible, and whether they require additional safeguards not provided for in these Guidelines, a case-by-case analysis is indeed necessary and the policy on any such proposed video-surveillance is subject to impact assessment and prior checking by the EDPS. However, as also noted in Section 5.8 of the Guidelines, where -as in the case of ECA- a system is set up for typical security purposes, the video-recordings *can* be used to investigate any physical security incident that occurs, for example, unauthorised access to the premises or to protected rooms, theft, vandalism, fire, or physical assault on a person. Indeed, in addition to deterrence and prevention, the video-surveillance system almost always also serves the purposes of investigating the facts after the occurrence of a security incident, and obtaining evidence to prosecute the perpetrator.

Provided the ECA's video-surveillance system is not deliberately installed or designed for the purposes of internal investigations beyond physical security incidents such as those noted above, it would -based on the information provided in the notification- not require ex-post prior-checking in the light of investigative purposes pursued.

b) *Employee monitoring and processing of special categories of data*

Whilst the notification form itself does not refer to any such purposes, the ECA Video-surveillance policy in its section 5 notes that "*...there are also cameras at the entrance to the computer room, inside the computer room and in the fitness room*", which could -in principle- be used for monitoring the work of staff or, as regards the fitness room, data concerning health.

However, the ECA Video-surveillance policy in its section 6.3 explicitly notes that "*The system is not used for any other purpose, for example, it is not used to monitor the work of employees or monitor attendance*" and its section 6.6 excludes the collection of special categories of data. This is further supported by the reasons given in the documentation submitted together with the notification for the two cameras:

- according to section 1.3.1. of the Privacy Impact Assessment and section 4 of the notification form, video-surveillance in the fitness room serves "*to establish whether persons exercising on their own have suffered an accident or malaise*". From the Video-surveillance audit report (section 29), which notes that "*Tests showed that sometimes one can recognise people within a distance of six metres from the camera. In all other cases one sees there is a person in the room but one is unable to identify the person*", it would further seem apparent that the camera installed in the fitness room is unsuitable for such a purpose;
- [...] section 6.2 of the ECA video-surveillance policy describes video-surveillance inter alia as "*...part of the measures to support the ECA's broader security policies*" which "*...helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to...IT infrastructure...*" and "*...helps prevent, detect and investigate the theft of equipment or assets owned by the ECA*".

Based on the information provided in the notification as submitted, the ECA's video-surveillance system would thus not require ex-post prior-checking in the light of employee monitoring and processing of special categories of data.

c) *Monitoring areas under heightened expectations of privacy*

Under the Guidelines, Section 6.8, "areas under heightened expectations of privacy" typically include individual offices, leisure areas, toilet facilities, shower rooms and changing rooms. In this context, it should be noted that "leisure areas" include sports facilities unrelated to an institution's mission such as the fitness room of the ECA[2]. Section 6.8 of the Guidelines notes that areas under heightened expectations of privacy should not be monitored and any derogation from this exception requires an impact assessment as well as prior checking by the EDPS.

The processing operations under examination are thus subject to ex-post prior-checking in conformity with Article 27 of the Regulation. However, as has been highlighted by the EDPS upon publication of the Guidelines[3], only in exceptional cases will the prior-checking be comprehensive and cover *all* aspects of a video-surveillance system. In most cases, the EDPS will *not* comprehensively review all aspects of the institution's video-surveillance practices.

Instead, as in the case at hand, the EDPS will usually focus his recommendations on those aspects of video-surveillance which differ from, or are in addition to, the common practices and standard safeguards set forth in the Guidelines (here the video-surveillance of the fitness room as monitoring of an area under heightened expectations of privacy).

2. Proceedings

[2] The updated version of the ECA Video-surveillance policy (submitted on 7 November 2011) in section 5 is in line with this assessment.

[3] See "Frequently asked questions on video-surveillance: prior checking", Section 5, available under http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_FAQ_videosurveillance_EN.pdf.

The procedure was notified for prior checking under Article 27 of Regulation (EC) No 45/2001 on 26 October 2011. According to Article 27(4) of the Regulation, the present Opinion must be delivered within a period of two months. The procedure was suspended for a total of 7 days (by email of 31 October 2011, until the submission of additional annexes to complete the notification on 7 November 2011) and 4 days for comments. Consequently, the present Opinion must be delivered no later than 9 January 2012.

3. Fitness room: monitoring an area under heightened expectations of privacy

Facts: As outlined above, the fitness room of the ECA is a "leisure area" in the sense of Section 6.8 of the Guidelines and as such an area under heightened expectations of privacy which should, in principle, not be monitored under the Guidelines.

- According to section 1.3.1. of the Privacy Impact Assessment and section 4 of the notification form, video-surveillance in the fitness room serves "*to establish whether persons exercising on their own have suffered an accident or malaise*".
- The Privacy Impact Assessment (sections 6.3 and 1.10 respectively) further notes in this respect that "*The only privacy risk which was identified is the fact that the images recorded by the camera installed in the fitness room, which can identify the persons exercising within 5 metres of the camera, could be used to spy on these sports enthusiasts. The risk was considered to be acceptable by senior management*." and that "*The Staff Committee has asked questions about the appropriateness of this camera and if the full-time presence of a fitness trainer/security guard is not a better alternative*".
- [...]

Recommendation:
From the point of view of privacy by design and as noted in Section 6.4 of the Guidelines, "*...when identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognisable facial images are captured*". For the purpose of ensuring help by the security personnel in case of an accident or malaise in the fitness room, it is not necessary to recognise people within a distance of six metres from the camera. ECA should consequently technically ensure that in all cases one can only see that there is a person in the room, but one is not able to identify that person.
Lacking further information, the EDPS is not in a position to assess the security implications of the full-time presence of a fitness trainer/security guard and its effectiveness compared to video-surveillance in this case. However, from a data protection point of view, it would seem that the direct supervision/recognition by a fitness trainer/security guard present on-the-spot is more invasive than video-surveillance without identification possibilities as recommended.

4. Reminders regarding other aspects of the ECA video-surveillance policy

a) Retention period

Under Section 8 of the ECA video-surveillance policy, the normal retention period for footage from the K1 and K2 buildings is 16 days and thus longer than recommended in Section 7.1 of the Guidelines. According to the Video-surveillance audit report, "*This is justified by the fact that the ECA closes completely over the Christmas and New Year period and the staff responsible for physical security are unavailable. To permit these people to investigate a physical security incident the images need to be kept for the maximum period the ECA is closed plus five working days to allow searches for images, their copying and/or transfer*".

As previously clarified by the EDPS[4], unless institutions provide sufficient justification and adequate safeguards, they should reduce the retention period to seven days or less, as recommended in the Guidelines. It would seem that other bodies have found technical solutions to bridging the period between Christmas and New Year. At any rate, specificities regarding a *once-a-year* event can hardly justify a prolonged *standard* retention period. The EDPS consequently invited the ECA to reconsider the current 16 days retention period.

[...]

c) On-the-spot notice and public version of the ECA video-surveillance policy

Section 5.1.2 of the Guidelines foresees that the purposes of the system must be communicated to the public on the spot in a summary form and in more detail, for example, via the public on-line version of the Institution's video-surveillance policy.

- As indicated by the Video-surveillance audit report (findings 10, 24, 27): the ECA should ensure transparency on its video-surveillance policy and the summary leaflet on the dedicated intranet and internet pages (links referring to the video-surveillance policy and the summary leaflet should actually redirect to these documents).
- The on-the-spot notice mentioned in section 9.1 of the ECA video-surveillance policy does not meet all content requirements stipulated in Section 11.2 of the Guidelines. The ECA should revise the notice so that it provides a link to the on-line video-surveillance policy (links should actually redirect to the video-surveillance policy). As indicated in the Video-surveillance audit report (findings 25 + 26) and as stipulated the ECA video-surveillance policy (section 9.1), an on-the-spot notice must be "displayed next to the areas monitored". Whilst under Section 11.2 of the Guidelines, it is not mandatory to place a notice next to every single camera, the EDPS invites the ECA to ensure that signs are adequately placed and are big enough that data subjects can notice them before entering any monitored zone and can read them without difficulty.

5. Conclusions

The EDPS recommends that the ECA adopts specific and concrete measures to implement the above recommendation regarding the video-surveillance in the ECA fitness room.

As concerns the reminders mentioned in this note, the EDPS would like to be informed about the situation regarding the compliance with the Guidelines and receive the requested information.

To facilitate our follow-up, it would be appreciated if you could provide the EDPS with all relevant documents within 3 months of the date of this letter which prove that all recommendations and reminders have been implemented.

Kind regards,

Giovanni BUTTARELLI

[4] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf