17 March 2010

EDPS Video-surveillance Guidelines

Summary of comments received on the 7 July 2009 consultation draft

Introduction: the consultation process

The EDPS published a consultation draft of their Video-surveillance Guidelines on 7 July 2009 and invited written comments by 15 September 2009 from Community institutions and bodies.

The following 13 institutions and bodies provided written comments:

1. Commission
2. European Anti-Fraud Office (OLAF)
3. Council
4. European Parliament (EP)
5. European Economic and Social Committee (EESC)
6. Committee of Regions (CoR)
7. European Court of Justice (ECJ)
8. European Court of Auditors (ECA)
9. European Central Bank (ECB)
10. European Chemicals Agency (ECHA)
11. Frontex
12. European Railway Agency (ERA)
13. Joint Research Centre in Ispra (JRC-ISPRA).

In addition, comments were received from the Data Protection Commissioner of Mecklenburg-Western Pomerania (Germany) and the British Computer Society (UK).

In several cases the three main groups of stakeholders - security services, data protection officials (DPOs) and staff representatives - commented in separate documents reflecting their specific points of view. For example, the Staff Committees of the ECB, CoR, as well as the Commission's Central Staff Committee each commented separately.

The consultation also triggered inter-institutional discussions. The DPOs of the Commission, OLAF, the EP and the Council provided a coordinated set of comments. The security services of the Commission, EP, EESC, CoR and the Council also provided joint comments.

On 30 September 2009 the EDPS held a workshop in Brussels on video-surveillance. Nearly a hundred DPOs and other data protection professionals, security officers, video-surveillance and IT specialists, and staff representatives from over forty Community institutions and bodies participated. In addition to the 13 institutions and bodies who had submitted written comments, several other institutions contributed to the debate, including:

1. European Training Foundation (ETF)
2. Office for the Harmonization of the Internal Market (OHIM)
3. Research Executive Agency (REA)
4. European Investment Bank (EIB)
5. Eurojust
6. European Centre for the Development of Vocational Training (Cedefop).

Following the workshop the EDPS invited participants and all DPOs to submit final comments by the end of October 2009. On 23 October 2009 the security services of seven institutions and bodies (EIB, Translation Centre, CoR, EESC, Council, ECA, EP) submitted a revised set of joint comments. Another European Community agency, Fusion for Energy, commented separately on 29 October 2009. On 13 November 2009, the Commission's security service also submitted a set of comments.

On 11 and 13 November 2009, the EDPS held follow-up meetings with the "DPO Quartet" (with the Commission, Council and OLAF DPOs present at this time), as well as with the representatives of those security services who expressed an interest in further clarifying and discussing the joint comments received from the security services of seven institutions and bodies on 23 October 2009.

Overview of the comments received

The consultation process achieved its two goals, namely:

- eliciting feedback to improve the draft Guidelines
- increasing cooperation to ensure compliance with data protection principles.

The overall response to the Guidelines was positive. Participants welcomed that the Guidelines provide practical advice for deciding whether or not to install or use video-surveillance equipment and when using, how best to address data protection issues.

However, important concerns were raised regarding key issues such as:

- the procedural framework for privacy by design
- accountability
- local decision-making
- the legal value of the Guidelines
- applicability of the Guidelines to existing systems and transitory provisions.

Stakeholders, including DPOs, requested further clarification on key “compliance tools” such as the video-surveillance policy, self-audit and impact assessment and warned against the risk of creating additional administrative burdens. In particular, the EDPS was asked to elaborate the added benefits of the new compliance framework and how it can fit into the existing system of notifications to the DPOs and prior checking by the EDPS.

Security services also voiced significant concerns. They insisted on the need to preserve their discretion to manoeuvre in key areas. Their main concerns were to

ensure that the Guidelines did not hamper them in carrying out their “mission” and were not overly prescriptive. They stressed the need to be able to keep their discretionary powers on what can be considered lawful and proportionate purposes for video-surveillance (in other words, how to define “security purposes”) and how long images can be retained. Some contributors emphasised that video-surveillance should be allowed to be used for very different security purposes, which should be defined broadly to allow flexibility. Special concerns were also raised with regard to particular security needs in response to terrorist threats. There was also a tendency for a more cautious approach regarding transparency and - at times - wishes were expressed to reduce the role and scope of staff consultations. There was also some reluctance expressed with regard to investment in privacy-enhancing technologies.

In terms of form, contributors welcomed that the Guidelines are written in plain language and in a user-friendly style, and contain helpful examples, which are especially useful for small agencies. At the same time, some contributors suggested shortening the Guidelines (without removing the examples and the specific recommendations).

With regard to the procedure leading to the finalisation of the Guidelines and further cooperation with stakeholders, different procedural options were suggested and opinions varied as to the necessity of a second round of comments. A formal working group procedure was considered by many as too “heavy”. On the other hand, others wished to go further and suggested the involvement of inter-institutional bodies such as the Inter-institutional Security College (Collège Interinstitutionnel de Sécurité).

Ultimately, the EDPS concluded that follow-up with the DPO Quartet, according to the Quartet’s usual procedures, and additional informal opportunities for clarifications would be sufficient and more productive at this stage. At the same time the EDPS offered anyone the opportunity to clarify or further discuss their comments. Furthermore, once the Guidelines are issued, the EDPS will:

- remain open to further cooperation with DPOs, the security services and other stakeholders

- provide further guidance on how to implement the Guidelines in practice.

For the compliance efforts to be successful, DPOs encouraged the EDPS to engage the management of the Institutions at the highest levels and send a strong message regarding the need to comply with the requirements presented in the Guidelines.

On a more general level, some contributors asked whether it is also the intention of the EDPS to follow this "new" procedural scheme - based on privacy by design, accountability of the institution concerned, and transparent local decision-making with the involvement of stakeholders - for other types of processing operations.

Summary of comments

The following summarises the main comments received on the draft Guidelines together with a reference to the Sections of the consultation draft of the Guidelines.

Legal value of the Guidelines (Section 1). Contributors requested further clarifications on the *legal value* of the Guidelines. Some security services suggested that the Guidelines should remain a non-binding collection of best practice. Other stakeholders, in particular, staff representatives, on the contrary, suggested the adoption of a legally binding document by European legislature, similar to video-surveillance laws adopted in some Member States, to ensure enhanced clarity and further protection to the individuals under surveillance. As a separate issue, some also pointed out that the practice of the European Court of Justice is that when an authority issues guidelines, it binds itself to them. Finally, contributors requested further clarifications on, and at times, questioned the legal basis for the obligations. DPOs therefore suggested that it will be difficult to "sell" the Guidelines to their institutions.

Definition of the security purpose (Section 2.2). Security services emphasised the need to retain their discretion on how to define the security purpose and for what security purposes video-surveillance can be used. They also emphasised that the *primary* purpose of video-surveillance should not necessarily be prevention, it can also:

- be a deterrence
- support investigations after the facts,
- support the process of securing evidence.

Some DPOs, on the other hand, suggested that the Guidelines should provide more specific guidance with respect to specific permitted and unlawful purposes by providing examples that address border-line and problematic cases. There are many additional uses which can be considered "useful" but are not permissible. Some claimed that in the document the wording is rather vague: "the EDPS discourages" certain uses.

Staff representatives emphasised that video-surveillance footage should not be used for data mining.

Data protection and privacy impact assessment (Section 3.2). DPOs suggested that the respective scope of the privacy and data protection impact assessment and of prior checking should be clarified, considering especially that the types of issues that require an impact assessment, usually, but not always, also require prior checking.

Privacy-friendly technologies (Section 3.3). With regard to privacy-friendly technological solutions, some commented that they are expensive and at present many of the institutions do not have them. It was also noted that requiring the use of such technologies would lead to distortion of competition and would make it more difficult to procure systems that are in other respects offer the best quality at an affordable price.

Consultations with stakeholders, including staff representatives (Section 4.2). Staff representatives welcomed the Guidelines and expressed interest to being involved and working together with other stakeholders as well as with the EDPS. As the Guidelines are flexible, and much depends on the details of implementation, they emphasised the need to keep a close eye on how they are implemented in practice. As

to who should represent staff concerns, opinions varied, with some favouring representation by Staff Committees, others advocating a more flexible approach, allowing, for example, representation by trade unions or the use of other existing decision-making structures.

Monitoring on Member State territory and in third countries (Sections 6.5 & 6.6). With regard to monitoring on Member State territory some security services suggested a "global approach" by the EDPS to ensure that the EDPS actively participates in dealing with local authorities. For Belgium, there is a suggestion to formalise an agreement with the Belgian government/police. It also seems that some security services use/wish to use PTZ cameras to single out known trouble-makers in crowds during demonstrations to help prevent violent attacks. Sometimes security services also allow/wish to allow national police direct access to CCTV. The special concerns at European summits and the need for protecting certain buildings from terrorist attacks were also emphasised. Further, a "global approach" was also suggested for third countries.

Others suggested that the Guidelines should be clearer on the "conflict of jurisdiction" issue. The important question is to identify the data controller. If an EU institution, then the processing falls under the scope of EU law. The reference to national DPAs in the Guidelines might suggest that they have jurisdiction whereas in reality - the contributors claim - it is a courtesy and the jurisdiction of the national authority is excluded.

Monitoring areas under "heightened expectations of privacy" (Section 6.8). With regard to these areas (where monitoring, in principle, is prohibited, and in any event, subject to prior checking), some security services want to remove "individual offices" from the list.

Covert surveillance (Section 6.11). Some security services insist on the need for covert surveillance for purposes such as investigating vandalism, theft, and spying. They agree that procedures are needed but want the EDPS to specify that the director of security in each institution has the power to order the use of covert surveillance (i.e. they want the director of security to be included specifically as a "competent senior decision-making body of the Institution").

Retention period (Section 7). Some security services wish to retain footage for 90 days. Other security services commented that 30 days would be sufficient and reasonable. On the other hand, staff representatives noted that even the one week general recommendation in the draft Guidelines is too long, arguing that the longer the images are kept, the greater the risk of misuse. For the general retention period, one justification put forward is that complaints at times come in after the retention period has expired. Special concerns to retain footage longer were raised with regard to some banking activities, classified information, nuclear sites and research laboratories.

In case the footage is needed for evidence, some security services want to keep the relevant footage for 10 years (referring to the Belgian statute of limitation for criminal procedures).

Registers of transfers and retentions (Sections 7.2 & 10.5). Security services understand the need for these compliance tools but some view it as an additional administrative burden noting that at least for police transfers, the "investigation report" would already have the information, albeit in a different form.

Access to recordings (Section 8). Some commented that outsourced personnel currently have no individual passwords and this should not be required as they have no access to advanced features on the system.

Data protection training (Section 8.2). Concerns were raised both on the DPO side and on the part of staff representatives about how can one judge the issues that one cannot technically understand. Contributors emphasised the importance of training not only on data protection issues to technical and security personnel, but also the importance of training for DPOs and other stakeholders such as staff representatives on the technical aspects of video-surveillance.

Access requests by the public (Section 12). Security services emphasised the exception for the case if access would harm the investigation. Some were of the opinion that no access to natural persons should be given, and the footage should be reserved for the police or judicial authority. (Access to natural persons then will be given by police or judicial authority according to their own rules on access.) Some security services also requested the EDPS to clarify what is meant by a "reasonable amount" that can possibly be charged for access.

Transparency vs confidentiality of the video-surveillance policy (Section 13.1). The principle of transparency was welcomed by many contributors. Staff representatives especially welcomed this principle as one allowing an informed debate, and helping to prevent, for example, the unlawful use of covert surveillance. At the same time, practical questions arose. For example, should the location of cameras be made public? Or should this information rather be made available only to designated staff representatives during the consultation process and possibly only in a summary form?

Data protection compliance audit (Section 13.2). Some DPOs initially suggested that the requirement for a compliance audit should be deleted on grounds that the standard (and prior) notification procedure is the regular opportunity for the DPO to check the intended processing operation against data protection requirements. They also noted that if the requirement is kept, it should be clarified what department should carry out an in-house data protection impact assessment: the DPO, the internal auditor or another one. Subsequently, it was further suggested that the involvement of the internal auditing services should be encouraged although this should not be to the detriment of the DPO's independence.

Transitory period (Section 15). Most contributors were concerned that the six-month transitory period is too short. Some suggested that one year would be sufficient. Others suggested a case-by-case approach where each institution could reach compliance according to its own internal timetable, to be discussed and agreed individually with the EDPS. Some raised the issue of the coming into force of the Lisbon Treaty and the general "business" of the coming months as an additional justification for a more gradual approach.

In the context of transitory provisions staff representatives underlined the importance of the fact that the Guidelines will not be only applicable to future systems but also to existing systems.