Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines

Table of Contents

Executive Summary

In March 2010, the European Data Protection Supervisor (EDPS) issued **Video-Surveillance Guidelines**[1] (Guidelines) based on the powers conferred on him in Article 47(1)(a) of Regulation 45/2001.

This public Report is a systematic and comparative analysis of the status reports received from a total of 42 European Union institutions and bodies (henceforth: bodies).

Next to highlighting best practices this report underlines shortcomings in those bodies lagging behind in their efforts to ensure compliance with the Guidelines. It furthermore clarifies certain aspects of the Guidelines, where questions were raised by bodies in preparing their video-surveillance policy or a need for clarification became apparent through the analysis of the state-of-play reports.

The EDPS takes note of the considerable efforts undertaken by those bodies which have submitted their state-of-play reports and is reassured that the Guidelines contributed to help raise the level of awareness and transparency regarding video-surveillance matters within the bodies. At the same time, more than a year after the adoption of the Guidelines and nearly two years after having started the consultation process, the EDPS is disappointed to see that the implementation of the Guidelines has been put on hold or significantly delayed in several bodies.

As an expression of their institutional accountability and good administration, bodies need to comply and demonstrate compliance with the Guidelines. As a supervisory authority, the EDPS must and will ensure that they do.

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

Part 1: Introduction

In March 2010, following a consultation process started in July 2009, the European Data Protection Supervisor (EDPS) issued **Video-Surveillance Guidelines** (Guidelines) based on the powers conferred on him in Article 47(1)(a) of Regulation 45/2001[2] (Regulation).

> The objective of these Guidelines is to offer practical guidance to the European Union bodies and bodies on how to comply with the law and use video-surveillance responsibly with effective safeguards in place. In setting out the principles for evaluating the need for its use, the Guidelines give guidance on how to conduct video-surveillance in a way which minimises impact on privacy and other fundamental rights. The Guidelines apply to video-surveillance systems already in place as well as to systems to be installed and activities to be carried out in the future.

Timing of this Report. Following a nine-month transitory period, the European Union institutions and bodies (bodies)[3] had until 1 January 2011 to bring their existing practices in compliance with the Guidelines and to provide the EDPS with state-of-play reports on their compliance status. This public Report is a **systematic and comparative analysis of the status reports received from a total of 42 bodies**[4]. 31 October 2011 is the cut-off-date for this report; although some bodies had indicated future steps towards compliance shortly before or some time after this date, the exercise was conducted strictly paper-based (i.e. limited to the documentation actually received by this date).

Preparation and scope. It is fair to state that the quality of the documentation submitted and the level of compliance achieved is as heterogeneous as the type of the bodies reporting: they range from small executive agencies with no video-surveillance or only a few cameras to EU bodies with seats spread over several Member States and well over one thousand cameras.

The EDPS is aware that many bodies made considerable efforts to ensure compliance and the personal efforts of many actors at different levels went into this. Wherever possible, the EDPS has tried to facilitate these efforts, e.g. by advising bodies at their request on specific issues regarding the implementation of the Guidelines.

As previously publically announced, next to **highlighting best practices**, this report also does underline shortcomings in those bodies lagging behind in their efforts to ensure compliance with the Guidelines. As noted in Section 1 of the Guidelines, they are primarily "addressed to those who decide whether to install video-surveillance systems and are responsible for their operation

[2] Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[3] See **Annex 1** for an alphabetical list of the institutional acronyms.

[4] Thirteen institutions reported to the EDPS within the 1 January 2011 deadline (some providing only an interim state of play), five with a delay of less than two months and eleven more over the course of March 2011. One body replied only in September 2011.

(the "controllers" in data protection terms[5])". Where *bodies* are being flagged as not complying with the Guidelines, this should therefore not necessarily be understood as a criticism of the (for the most part considerable) compliance efforts undertaken by that body's Data Protection Officer (DPO).

This report furthermore clarifies certain aspects of the Guidelines, where questions were raised by bodies in preparing their VS policy or a need for clarification became apparent through the analysis of the state-of-play reports.

Overall appreciation. The EDPS takes note of the considerable efforts undertaken by those bodies which have submitted their state-of-play reports and is reassured that the Guidelines contributed to help raise the level of awareness and transparency regarding video-surveillance matters within the bodies.

- **Participation**: This analysis relies on the status reports received from a total of 42 bodies. Out of those 29 bodies which control the operation of their CCTV system, 13 reported to the EDPS within the 1 January 2011 deadline, five with a delay of less than two months and eleven more over the course of March 2011.
- **Limited use of "intrusive" CCTV**: Twelve bodies explicitly exclude the use of "high-tech" or intelligent CCTV and no body reports the use of sound recording and “talking CCTV”.
- **"Privacy by design"**: In reporting on their state-of-play, additional bodies have confirmed their efforts in the use of privacy-friendly technological solutions, e.g. in blurring certain images, in avoiding technically that recognisable features are captured where the recognition of individuals is not necessary or through the selective activation of cameras by motion detection.

At the same time, more than a year after the adoption of the Guidelines and nearly two years after having started the consultation process, the EDPS is disappointed to see that the implementation of the Guidelines has been put on hold or significantly delayed in several bodies.

- **Content of the on-the-spot notice**: The level of compliance is limited: only two bodies meet all requirements. This is surprising, as Appendix 2 of the Guidelines contains a sample on-the-spot data protection notice.
- **Publication of an online video-surveillance policy**: Out of the 18 bodies having provided (draft) policy documents, *all* claimed in their policy to have published their policy or a limited version of it online. When testing access, the EDPS found that only three bodies provided relevant information and one of a very limited scope.
- **Impact assessments** (IA): Only five bodies announced an IA for the future or noted that an IA was currently ongoing. In this context, the

[5] Article 2(e) of the Regulation.

EDPS is concerned about the lack of statistical or even anecdotal evidence underlying the bodies' decisions to put video-surveillance into place. In the absence of an evidence based risk analysis relying on actual security incidents, it seems very difficult for bodies to convincingly make the case for using video-surveillance.

- **Data protection training**: Only eleven bodies reported that an initial training had taken place and only seven bodies clearly confirmed that external staff had been covered by training activities. The EDPS consequently urges all bodies which have not done so yet to provide all personnel with access rights, including outsourced personnel with data protection training and familiarize them with the provisions of the Guidelines insofar as these are relevant to their tasks.

As an expression of their institutional **accountability and good administration**, bodies need to comply and demonstrate compliance with the Guidelines. As a supervisory authority, the EDPS must and will ensure that they do. Part 4 of this Report contains an outlook on following steps.

Part 2: Terms of reference

Under Section 15 of the Guidelines, the status of compliance with the Guidelines was to be notified by each body in a letter to the EDPS (the "**state-of-play report**") in which the respective DPO confirms that the body has adopted a video-surveillance (henceforth: "VS") policy and carried out an audit and specifies whether the body also carried out an impact assessment; and whether the body believes that an ex-post prior checking is necessary, and if so, on what grounds.

Section 15 of the Guidelines also noted that "If, despite the best efforts by an body, compliance on certain, specific items cannot be reached by the **1 January 2011 target date**, the body should adopt a plan committing itself to full compliance using a step-by-step approach and submit it to the EDPS by 1 January 2011, along with the rest of the documents listed above".
Thirteen bodies reported to the EDPS within the 1 January 2011 deadline (some providing only an interim state of play, some giving indications as to their step-by-step approach), five with a delay of less than two months and eleven more over the course of March 2011. One agency (GSA) replied only in September 2011.

What kind of documentation underlies this report?

As has been pointed out above, the quality of the documentation submitted is as heterogeneous as the type of the 42 bodies reporting. Two bodies reportedly have no VS system in place at all, one body has a "deactivated" system and ten bodies do not actually control the VS system operating on their premises.

Under Section 15 of the Guidelines, in order to carry out this ex-post review in the most efficient manner, the EDPS recommended a global approach, whereby each institution carries out a single exercise in which:

- it verifies (either in a formal audit or in an informal fact-finding exercise) the adequacy and compliance of existing practices against the Regulation and the Guidelines;
- prepares (or updates) the Institution's **VS policy;**
- audits the revised practices against the revised policy, the Guidelines and the Regulation in a formal adequacy and compliance **audit**.
When necessary or helpful, an ex-post **impact assessment** should also be prepared as part of the same review.

Policy documents. From the remaining 29 bodies, 14 provided us with a formally adopted policy document[6] and four provided draft policy documents. Out of the 18 (draft) policy documents received, twelve were based on the template provided as **Appendix 1 of the Guidelines** ("Sample video-surveillance policy"). One body (ECHA) explicitly noted that its policy is "not a simple copy-paste version of the sample attached to the EDPS Guidelines, but has been carefully adapted to the reality and the needs" - an approach the EDPS would like to encourage.

Whilst relying on the template is certainly not mandatory and does not in itself represent a guarantee for compliance with the Guidelines, those who used the template to formulate their policy tend to do better in terms of compliance. The EDPS would consequently recommend that those bodies which have not yet provided a policy document make use of the template provided in the Guidelines for that purpose. Best practice examples regarding the use of that template are the ECB for its future premises as well as the EEA. Unfortunately (see Part 3, section 14: "Publication of an online policy"), both policy documents are currently not publically available.

Section 13.1 of the Guidelines notes that the bodies should make their video-surveillance policies publicly available on their intranet and internet sites. If these documents contain confidential information, then a non-confidential version should be made publicly available. Twelve bodies opted for a separate, more limited / **restricted public version** of the policy document. A best practice example of such a restricted public version is the CPVO's policy.

More than a year after the adoption of the Guidelines and nearly two years after having started the consultation process, however, some bodies still have no (draft) policy (see in particular Part 3 of this Report).

Audit documentation. Out of the 20 bodies which have conducted an audit (compliance and / or adequacy) or plan to do so in the future, only very few have provided the EDPS with the relevant documentation.

Under Section 13.2 of the Guidelines, each institution should verify and document the compliance of its practices with the provisions of the Regulation, the Guidelines and its own VS policy in a data protection audit. The objectives of this audit exercise are twofold:

- to verify that there is a documented and up-to-date VS policy in place and that this policy complies with the Regulation and the Guidelines (**adequacy audit**); and

[6] One institution provided us with two policy documents (for its existing as well as its future premises, which are currently under construction).

- to check that the organisation is in fact operating in accordance with is VS policy (**compliance audit**).

The EDPS had previously noted[7] that based on documentation submitted alone, it is not always in a position to determine the actual extent of compliance by the bodies concerned. On the one hand, the EDPS cannot exclude that those bodies which did not undergo any form of audit might have -at least partially- gotten away with paying lip-service to actual compliance by cutting and pasting the policy template contained in Appendix 1 of the Guidelines. On the other hand, those bodies which have "played by the rules" and undergone a full-fledged audit might now find themselves with audit findings that -under these circumstances somewhat "unfairly"- represent them as partially non-compliant with the Guidelines.

To ensure transparency, and also to enable the EDPS to effectively carry out his supervisory role, the EDPS therefore encourages all bodies concerned to not only adopt a comprehensive VS policy, but also to carry out an audit, as provided in the Guidelines. Future **thematic on-site inspections by the EDPS at selected bodies cannot be a substitute** for a data protection (self-) audit.

Of those audit documents provided, only five contained all elements required by the Guidelines (see box below) and were also comprehensive with regard to an assessment of both compliance and adequacy for the entire body. Examples: one audit report consisted of only 1 page; another audit report covered only two out of three seats of the body.

Section 13.2 of the Guidelines notes that the audit report should:
- record date, scope, members of the audit team, etc.,
- summarise the main findings of the audit and any non-compliances identified,
- document suggestions for any corrective action, and
- record the nature and timescale of any agreed follow-up.

Only seven bodies made use of **on-site visits** or plan to do so in the future. This is a pity, as the EDPS had previously recognized[8] the added value of such an approach, e.g. in the context of assessing proportionality of the cameras' locations and viewing angles on the premises and recommended that this verification should be carried out by each body, in the framework of a formal audit. One body (EEA) conducted a self-audit by the DPO together with staff. In the light of the constructive results resulting from this exercise, the EDPS encourages the active **participation and involvement of staff** in the audit process.

The Guidelines (Section 13.2) note in this respect that "Some of the adequacy audit can be conducted off-site, based on written documentation. However, for a full audit, it is vital to

[7] See: Follow-up to video-surveillance guidelines: summary of preliminary recommendations in nine prior checking procedures, 14 July 2010 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf.

[8] See footnote 7.

also carry out on-site visits, review video-surveillance software and hardware, on-the-spot data protection notices, data retention and transfer registries, log files, access requests and other documentation available on the use of the system, and conduct interviews with management and staff members".

Only seven bodies mention that the **Internal Audit Service** was conducting the audit or at least assisting the process (or was planning to do so in the future). Regrettably, one institution (EP) reported that the IAS did not respond positively to the DPO's request for participation.

The Guidelines in Section 13.2 note that "For self-audits, whenever possible, the EDPS recommends that the audit team should include the Institution's internal auditors and that they should receive adequate training on data protection and the Guidelines".

Two bodies explicitly mention that their in-house audit (self-audit) has been or is going to be carried out by their **security staff** - despite the recommendation in the Guidelines (Section 13.2) according to which, whenever possible, it should be ensured that the auditors are independent of the function being audited (typically, the security unit).

As further noted in the Guidelines (Section 13.2), the audit may also be carried out by an independent third party contracted for this purpose (**third-party audit**). One body (FRA) provided an assessment of its CCTV system undertaken by a security company (not the one in charge of security services at that body).

The Guidelines (Section 13.2) further noted that the third party auditor may be, for example, another body if the auditing is carried out on a reciprocal basis. In this case, the bodies audit each other's practices, which may encourage benchmarking and the adoption of best practice. Regrettably, this option of **reciprocal inter-institutional auditing** has not been used by bodies so far. The EDPS recommends the use of this "peer" auditing option for benchmarking reasons, in particular for all those bodies which would otherwise have to rely on their security staff and which, amongst the others, can identify a body with similar VS needs and/or VS policy.

Impact Assessments (IAs). As further outlined in Section 3.3 of the Guidelines, the EDPS recommends that a privacy and data protection IA should be carried out before installing and implementing VS systems whenever this adds value to the body's compliance efforts. The purpose of the IA is to determine the impact of the proposed system on individuals' privacy and other fundamental rights and to identify ways to mitigate or avoid any adverse effects. In any event and in all cases, whether in a formal IA or otherwise, the bodies must assess and justify whether to resort to video-surveillance, how to site, select and configure their systems, and how to implement the data protection safeguards proposed in the Guidelines.

Due to their complexity, novelty, specificity, or inherent risks, the EDPS recommends carrying out an impact assessment in the following cases (Section 3.3 of the Guidelines):
- VS for purposes other than security (including for investigative purposes);
- employee monitoring;
- webcams;

- monitoring on Member State territory and in third countries;
- special categories of data;
- areas under heightened expectations of privacy;
- high-tech and/or intelligent video-surveillance;
- interconnected systems;
- covert surveillance;
- sound-recording and "talking CCTV".

Section 5.6 of the Guidelines notes that even if a body concludes that there is a clear need to use VS and there are no other less intrusive methods available, it should **only use VS technology if the benefits outweigh its possible detrimental effects**.

One body reported that whilst audio recording and "talking CCTV" were technically feasible with some of their camera models, these options were not actually used in practice. Whilst the EDPS welcomes this decision, this case of over-calibrated equipment illustrates why it actually pays to consider privacy-friendly technology solutions before installing the systems.

Only five bodies announced an IA for the future or noted that an IA was currently ongoing[9]. This is regrettable given that in many cases, the above cost/benefit analysis would seem to be complex and the legitimate interests and rights of the people monitored may need to be balanced very carefully with the benefits that may be achieved by the surveillance.

Ten bodies at least report some kind of privacy related considerations in the context of establishing their VS policy. Given the impact of VS on fundamental rights of those monitored, this can hardly be considered satisfactory. As noted in Section 5.5 of the Guidelines: the mere availability of VS technology at a relatively low cost is not sufficient to justify its use. Bodies should refrain from simply making the choice which appears to be the least expensive, easiest and quickest decision but which fails to take into account the **impact on the data subjects' legitimate interests and the effect on their rights**[10].

In this context, the EDPS is concerned about the **lack of statistical or even anecdotal evidence** underlying the bodies' decisions to put VS into place. In the **absence of an evidence based risk analysis** relying on actual security incidents, it seems very difficult for bodies to convincingly make the case for using VS in the absence of properly documented IAs. Obviously, should this lack of statistical or even anecdotal evidence regarding security incidents result from the fact that such incidents are actually quite scarce at EU bodies, this should be considered very good news. However, this assumption of a no-/low-threat scenario would contrast with the argumentation of quite many bodies (in particular those which actually operate quite a lot of cameras.

[9] Two IAs have been provided to the EDPS.

[10] See Article 4(1)(c) of the Regulation and Articles 8 and 52 of the Charter of Fundamental Rights of the European Union. Other relevant provisions on fundamental rights include, among others, Articles 7, 11, 12, 21 and 45 of the Charter. See also the European Convention on Human Rights, in particular, Articles 8, 10 and 11 and Protocol 4, Article 2, as well as Article 19 of the Treaty on the Functioning of the European Union.

The EDPS understands that, sometimes, the size of the body or its VS system might indeed not warrant launching a full-fledged IA exercise (an argument expressly used by CPVO and EASA). It should, however, be noted that this should not hinder the body concerned to carefully consider the impact of the VS system in place.

Six bodies explicitly noted that they are due to move and four bodies announced a significant overhaul of their security system or a change in security provider in the not too distant future. The EDPS would like to highlight that a system overhaul or the move to a new building are indeed good opportunities for implementing a genuine "Privacy by design" approach.

Whose video-surveillance were we looking at?

Two bodies reported that they **have no video-surveillance system in place at all**. One of those noted that the system is "deactivated". Also with a view to those bodies that have been established only after the publication of the Guidelines, the EDPS would like to note that where **deactivated** VS systems are re-activated at a later date or installed for the first time, it is of course incumbent on the relevant controller to ensure an appropriate notification to the Data Protection Officer (DPO) prior to any possible notification under Article 27 of the Regulation to the EDPS[11].

The **40 remaining bodies have some kind of VS system in place** on their premises, with the vast majority (29) confirming that they possessed such system before the publication of the Guidelines in March 2010. One body (OSHA) introduced its VS system after the publication of the Guidelines, but before the due date of the state-of-play report (1 January 2011).

As noted in Section 14.2 of the Guidelines ("**Video-surveillance by third parties**"), at times, video-surveillance is not carried out by the body or a contractor on its behalf, but rather by the landlord from whom the body leases its premises or by a contractor on behalf of the landlord. In some cases there may be a complex contractual system involving several leases and subleases, and/or several contractors and subcontractors and the body may have little or no contractual influence on the operator of the video-surveillance system. **Eleven bodies reported that they were not controller** of the VS system in place, with most of these (ten) relying on VS systems operated by another EU body (COM, EP, EIB).

In this context, the EDPS would like to draw attention to **Opinion 1/2010 of the Article 29 Data Protection Working Party** on the concepts of "controller" and "processor" adopted on 16 February 2010[12] (WP 169, hereinafter: "WP29 Opinion"), which analyses, in detail, the issues of controller-processor relationships.
On page 11, the WP29 Opinion emphasizes that "The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis".
Page 12 the WP29 Opinion stipulates that "In case of doubt, other elements than the terms of a contract may be useful to find the controller, such as the degree of actual control

[11] Please see Part 3, section 3 "Consultations" and Section 4.3 of the Guidelines for indications as to when a notification to the EDPS of VS systems might be required.
[12] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility...".
On page 26, the WP29 Opinion specifies that "Parties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance".

As noted in Section 14.2 of the Guidelines, even though in most such situations the body will not be considered a "controller", it should take a proactive role and make reasonable efforts to ensure that the controller carries out VS in compliance with the Guidelines. In such cases, it is advisable that the body concerned raises any specific concerns regarding VS with the actual controller, and if it considers that the data processing activities of that controller are carried out in a way that infringes the Regulation, inform the EDPS accordingly[13].

The EDPS also emphasizes the following practical obligations incumbent on the "non-controlling" body:

- act in due diligence in reviewing the relevant practices of the actual controller;
- communicate the controller's practices to its staff and visitors (e.g. ensure that on-the-spot notices are posted and more detailed information is made available on the body's intranet and internet sites);
- raise with the controller (and ultimately, with the EDPS, if legality is at stake) any concerns it may have regarding the legality or customization of the controller's services as it deems necessary.

The EDPS recommends, in particular, that the "non-controlling" body assesses whether any particular provisions of the controller's VS policy should be modified to take into account the specific situation of the "non-controlling" body. For example, if the controller were to have a policy in place for covert surveillance, but a "non-controlling" body were to consider such a possibility unnecessary or disproportionate with respect to its own building, it should raise such concerns directly with the controller.

One body reported that it is situated in an office building provided by Member State authorities, who also provide CCTV and security services through a sub-contractor. As "non-controlling" body, its practical obligations are *mutatis mutandis* similar to those outlined above for inter-institutional situations.

What kind of video-surveillance were we looking at?

The level of technical sophistication of the equipment used and the extent to which use is made of it by the bodies seems to be, again, just as heterogeneous as the type of the reporting bodies.

Where numbers were provided, these range from over one thousand cameras institution-wide to several hundred cameras, several dozens or 25 or less. It is difficult to make a general assessment in the light of the various determinants

[13] In case the controller is not subject to Regulation 45/2001, but to the national law of a Member State giving effect to Directive 95/46/EC, this may involve the intervention of the competent national DPA.

of these numbers and based on the submissions alone. However, the audit findings for one institution remarkably include that controllers find it difficult to identify certain cameras given their sheer number[14].

Part 3: Assessing the level of compliance by topic

This part of the Report looks at particular topics as defined and in the order established by different sections of the Guidelines. In the light of each particular topic, it aims at identifying best practice examples and, where required, includes naming and shaming of bad performers.

1. The use of privacy-friendly technology

Section 3.4 of the Guidelines notes that whenever possible, privacy-friendly technological solutions should be used; when commissioning the system and drafting tender specifications, contractors should therefore be invited and incentivised to offer such solutions. The Guidelines mention two examples of such solutions: the encryption of data and the masking or scrambling of images.

The EDPS welcomed in an earlier Opinion[15] that an institution had confirmed that its cameras which are capable of panning, tilting and zooming are equipped with masking technology. As noted in that Opinion, this helps ensure that in those cases where it is inevitable that some private areas come into the field of vision of cameras, no images from those areas could be captured.

The EDPS encouraged other bodies on that occasion to upgrade their systems accordingly and in general, to make better use of privacy-friendly technologies and noted that this also includes the use of image-editing software to allow an organization to edit-out images of third parties when giving access to data subjects.

In reporting on their state-of-play, more bodies have confirmed their efforts in this respect. One reports that recording by cameras focussing on national territory is activated only if a mass movement towards that body's building has been detected. Another one notes that where the recognition of individuals is not necessary, the camera/object lens combination is chosen in such a way that no recognisable features are captured. At a third one, cameras in the vicinity of increased privacy areas are focussed and positioned so that these

[14] "Il est difficile pour les contrôleurs du dispatching d'identifier exactement certaines caméras car il en existe beaucoup...".
[15] See footnote 7.

areas are not monitored. A fourth reports that disks containing recordings of images are serial numbered and subject to watermarking.

Two bodies explicitly note that they did not find it necessary to consider the use of privacy-friendly technological solutions. Whilst the size of the body or its VS system might indeed not warrant elaborate technical solutions, under the Guidelines, bodies should be able to demonstrate that they have at least considered some of the low-tech options - or will consider those when updating their VS system. EASA's draft policy explicitly mentions the objective of ensuring that the VS system is designed with privacy and data protection concerns in mind and stipulates that future revision activities should try to implement privacy-friendly solutions whenever possible. The EP noted that it shall consider the use of privacy-friendly technological solutions when the current system is changed, upgraded or if any additions are planned.

One body reported that whilst audio recording and "talking CCTV" were technically feasible with some of their camera models, these options were not actually used in practice. As noted in Section 3.2 of the Guidelines, a privacy-by-design approach already at the stage of installing or updating a video-surveillance system, including an initial data protection assessment "well before a tender for new acquisitions is issued or any financial commitments are made...will help prevent costly mistakes".

2. Ad hoc surveillance

In line with Section 3.5 of the Guidelines, advance plans should be made where a body contemplates using VS on an ad hoc basis (for example at times of hosting high-profile events or during internal investigations). In this case the necessary framework and policies for data protection should be established sufficiently before the occurrence of the VS itself.

Ten bodies explicitly exclude the use of VS on an ad hoc basis; one excludes this currently, but reserves this option for the future. Four bodies do make use of ad hoc surveillance or reserve the right to use ad hoc VS under certain conditions. For example, one body notes that, provided ad hoc VS is "an effective countermeasure", it may be started if the Security Manager so decides, e.g. because of prominent guests, a temporarily increased security risk or because other physical systems are not functioning.

3. Consultations

Section 4 of the Guidelines highlights that consultation with stakeholders and competent authorities is essential in order to identify all relevant data protection concerns.

> For this purpose, Section 4 of the Guidelines suggests that when deciding whether to use video-surveillance and establishing the necessary framework and policies for data protection, some or all of the following individuals or organisations may need to be consulted:
> - the DPO of the Institution,
> - employee representatives,
> - other stakeholders (including, in some cases, local authorities),

- the EDPS and
- national (or regional) data protection authorities.

DPOs. Under Section 4 of the Guidelines, the plans to install or update a video-surveillance system should -first and foremost- be communicated to the DPO of the body, who should be consulted in all cases and should be involved in all stages of the decision-making. Most (if not all) DPOs seem to have been actively involved or at least consulted in the process of defining their body's VS policy and many will be implied in monitoring compliance in the context of self-audits in the future.

Staff and other stakeholders. In the Guidelines, the EDPS recommended that staff should be consulted[16] in all cases where staff members may be captured on cameras. This would seem to be the case in all reporting bodies[17]. Ten bodies reported explicitly having involved staff in defining their VS policy, two bodies note that such consultation is planned or ongoing.

Best practice examples include

- the EEA, where in the process of defining the VS policy, a self-audit was conducted by the DPO and with the active and seemingly constructive involvement of staff members;
- the CdT, which at the express request of its Staff Committee excluded the use of covert surveillance.

If there are other stakeholders present, due to the location or specific nature of the VS in place, the Guidelines further invite each body to ensure that those stakeholders or their representatives are also consulted as widely as possible. The state-of-play reports submitted do not refer to any such consultations or their result. The EDPS consequently invites the bodies concerned to verify that there are no other stakeholders who have so far not been given the opportunity to contribute to their VS policy. As pointed out by the Guidelines, this also includes consultation with local governments, police or other bodies in the cases referred to in Sections 6.5 and 6.6 of the Guidelines (see in particular Part 3, Section 9 of this Report on achieving compliance with retention periods).

EDPS. Section 4.3 of the Guidelines refers to the need to submit a prior checking notification under Article 27 of the Regulation to the EDPS only in some cases, noting that the aim of this procedure is to assist the body in establishing additional data protection safeguards in cases where its activities go beyond the standard operations for which the Guidelines already provide sufficient safeguards.

[16] The EDPS suggested consultation via the staff committees operating in the Institutions but noted that other means (e.g. public consultations and workshops) may also be effective.

[17] In an earlier Opinion (see footnote 7), the EDPS had already welcomed as good practice that one organization's notification confirmed that the organization consulted its staff when developing its video-surveillance policy and the EDPS had encouraged all other institutions and bodies to also follow the EDPS Guidelines in this respect.

Several bodies **notified "ex-post" prior checking procedures** to the EDPS, some of which had been submitted well before the publication of the Guidelines in March 2010[18]. As anticipated in Section 15.2 of the Guidelines, on 8 July 2010, the EDPS issued brief recommendations in nine ex-post prior checking procedures (regarding six bodies: COM, CoR, EESC, Council, CJEU, FRA) where the notifications were submitted prior to the publication of the Guidelines with a view to assist further the compliance efforts of the bodies concerned. To ensure transparency and facilitate comparison of best practice, the EDPS also published a summary of these recommendations[19].

As outlined in Section 4.3 of the Guidelines, the EDPS considers that a prior checking notification is required for the following cases (references are to the Sections of the Guidelines):

- video-surveillance proposed for investigative purposes (Section 5.8),
- employee monitoring (Section 5.9),
- processing of special categories of data (Section 6.7),
- monitoring areas under heightened expectations of privacy (Section 6.8),
- high-tech or intelligent video-surveillance (Section 6.9),
- interconnected systems (Section 6.10),
- covert surveillance (Section 6.11),
- sound-recording and "talking CCTV" (Section 6.12).

The notification must include the impact assessment report (or other relevant documentation on the impact assessment), the video-surveillance policy and the audit report.

Where the above requirements are fulfilled and a notification has been submitted after the publication of the Guidelines[20] (e.g. ECHA), Section 15.1 of the Guidelines anticipated that "*as of 1 January 2011, and upon receipt of the requested documentation, the EDPS will establish a schedule for the processing of the ex-post prior checking notifications. Depending on the number and quality of the prior checking notifications received, the range of issues encountered, and other relevant factors, the EDPS may issue individual opinions or joint opinions with respect to several Institutions and/or issues. The procedure may also include on-the-spot checks or inspections".*

However, considering the above criteria and in the light of the information supplied (as noted above: the evaluation underlying this Report was conducted strictly paper-based), some additional **prior checking notifications** would seem to be required, but remain to be submitted. Examples are (see also below, Part 3, Section 4):

- The use of covert surveillance by one body, where according to the draft policy "Covert video surveillance (use of webcams) is authorized under special circumstances, without PC with the EDPS, so that investigations cannot be compromised". The EDPS calls upon this body to carefully

[18] OLAF's CCTV system, which covers only the OLAF security perimeter, was prior-checked in case 2007-634.
[19] See footnote 7.
[20] In one case, a notification submitted after the publication of the Guidelines has been withdrawn after it was established that no prior checking notification was actually required under Section 4.3.

reconsider whether it wishes to avail itself of covert surveillance in the future and recommends that this evaluation should be carried out in the framework of a formal impact assessment and, subsequently, be notified for prior checking.

- Another body foresees the temporary set-up of cameras for internal investigations.
- Whilst in principle excluding employee monitoring, one policy nevertheless foresees this possibility "*à titre exceptionnel, sous réserve que...démontre qu'il est dans son intérêt supérieur de mettre en oeuvre cette surveillance*".
- The technical specifications of the cameras used in one body include references to a temperature sensor and motion detection.
- Another body operates infra-red detectors outside working hours to detect intruders.

In this context, the EDPS reiterates that in all cases where prior checking is necessary, **bodies must first carry out an impact assessment** and **submit their notification to the EDPS prior to the processing** of data.

It should also be noted that some bodies (TEN-T EA, ECB) have launched **consultations under Article 46(d) of the Regulation** on specific issues that arose in drafting their policy. The EDPS stands ready to help bodies with any specific problems in this context, but -in the presence of the very comprehensive Guidelines- will not "rubberstamp" entire VS policies.

National Data Protection Authorities. As noted in Section 4.4 of the Guidelines, whilst the EDPS is competent to supervise all VS carried out by or on behalf of the bodies, irrespective of whether they capture images within the buildings of the bodies or outside those buildings, the data protection authorities of the Member State in which the body is located may also have an interest with respect to monitoring that takes place outside the buildings[21].

Given that one body is of the opinion that no contacts must be established with the national authorities, it should be highlighted that the above mentioned notion of *monitoring* includes the monitoring of live images[22].

Eleven bodies report to have consulted the relevant national Data Protection Authority (DPA). On the need for further cooperation with national data protection authorities, see also Part 4.

4. The legitimate purpose of VS

Under Section 5.1 of the Guidelines, bodies must establish the legitimate purpose of their VS. In doing so, they need to be clear, specific and explicit - **vague, ambiguous or simply too general** descriptions are not sufficient.

[21] Section 4.4 of the Guidelines notes that in this case, the applicability of national data protection law is, in any event, limited by the privileges and immunity enjoyed by the Institutions pursuant to Article 343 of the Treaty on the Functioning of the European Union and Protocol (No 7) on the privileges and immunities of the European Union, Official Journal C 115, 9/5/2008, p. 266-272.

[22] As explicitly pointed out in Section 2.3.4 of the Guidelines, live video-monitoring or live video-broadcast also come under the scope of the Regulation and Guidelines.

Being specific about the purpose of the VS can help the bodies to comply with the law, assess the success of their system, and explain to their staff and members of the public why it is needed. Further, it must be ensured that the data are not subsequently used for unforeseen purposes or disclosed to unforeseen recipients who might use them for additional, incompatible purposes ("**function creep**"). Insofar as 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 body's video-surveillance policy, compliance would seem to be regrettably low (see Part 3, Sections 13 + 14 of this Report).

A total of 16 bodies have -in their (draft) policies or otherwise at least in a summary form- provided the EDPS with **clear, specific and explicit** indications as to the purpose of their VS system. As already pointed out by the EDPS[23], further efforts are necessary to ensure that the purpose is defined with sufficient clarity and specificity and that the surveillance efforts are sufficiently selective and targeted for all bodies using VS. In this respect, the EDPS had already emphasized that a thorough and specific risk assessment may greatly facilitate the accurate definition of the purposes of the system.

General security purposes

For roughly half of the 16 bodies having clearly defined the purpose of their VS system, this is limited to **general security purposes**. Apart from brief references in some state-of-play reports to demonstrations or the fact that cameras capturing physical characteristics of individuals might thus reveal their racial or ethnic origin, only one body referred to the processing of **"special categories of data"**. As the EDPS had previously noted[24], an IA focusing on this particular issue should be carried out and a prior checking notification should be submitted to the EDPS "when any **demonstrations** or protests are *regularly* held in the vicinity of the buildings and demonstrators/protestors may come within the field of vision of the cameras".

Two bodies specifically mention terrorism in the context of their security considerations, with one noting that the bodies are potential targets for terrorists or miscellaneous other groupings ("...*anarchistes, islamistes, extrémistes, etc.*").

As had been previously noted by the EDPS[25], each body should verify whether - beyond more general security purposes - it also uses VS for additional purposes for which an IA and prior checking may be necessary (see below).

Investigative purposes

Section 5.8 of the Guidelines stipulates that "where 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,

[23] See footnote 7.
[24] Ibidem.
[25] Ibidem.

vandalism, fire, or physical assault on a person. However, in principle, video-surveillance systems should not be installed or designed for the purposes of internal investigations beyond physical security incidents such as those noted above."...
"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 necessary. Therefore, your policy on any such proposed video-surveillance is **subject to impact assessment by your Institution and prior checking by the EDPS**". (emphasis added)

Five bodies[26] note that they use or have the intention to use their VS system for investigative purposes; eight bodies remain vague in this respect or do not explicitly exclude such purposes.

- One institution notes that it uses VS "as an investigative tool" and audit findings support that cameras are used for investigative purposes;
- An agency foresees the temporary set-up of cameras for internal investigations;
- Another agency intends to use footage in disciplinary proceedings in extraordinary cases, when the images captured demonstrate that there has been a failure to comply with the obligations incumbent on staff, and more in particular those set forth in the Staff Regulations and its implementing rules, the ... Code of Good Administrative Behaviour or the ... Security Rules, or when a suspected criminal offence is captured."

Employee monitoring

Under Section 5.9 of the Guidelines, the use of video-surveillance to monitor how staff members carry out their work should be avoided, apart from exceptional cases where a body demonstrates that it has an overriding interest in carrying out the monitoring. Against this background, the EDPS had previously particularly welcomed[27] one organization's notification (as well as the notice provided to data subjects) which clearly stated that VS will not be used for monitoring the work of employees.

Section 5.9 of the Guidelines further notes that "Overly intrusive monitoring measures can cause employees unnecessary stress and can also erode trust within the organisation... Therefore, any such proposed video-surveillance is subject to an **impact assessment** by the Institution. The Institution must also submit its plans to the EDPS for **prior checking**. .(emphasis added)

Based on the information provided in the state-of-play reports, several bodies are using or intend to use employee monitoring to a certain extent or under certain circumstances (ten others do not address or explicitly exclude such possibility). For example, whilst in principle excluding employee monitoring, the policy of one body nevertheless foresees this possibility "*à titre exceptionnel, sous réserve que...démontre qu'il est dans son intérêt supérieur de mettre en oeuvre cette surveillance*". This body clearly notes that the (currently abstract) possibility to use VS for employee monitoring will require an IA and two other bodies have provided their IA to the EDPS in this context.

[26] Two bodies have provided the EDPS with an IA in this context.
[27] See footnote 7.

Webcams

As highlighted in Section 5.10 of the Guidelines, "Webcams should normally not be installed for frivolous purposes, or to promote recreational facilities offered by the Institution or a tourist location (e.g. visitors centre, fitness centre, cafeteria, visitors' gallery in a meeting room). In exceptional cases the use of webcams may nevertheless be permissible based on the informed and individual consent of each user of the facility. ...Another important factor to consider when designing a system is the extent to which individuals are identifiable: a bird's eye view of a building with low-resolution is much less intrusive than images where the faces of the individuals can be recognised."

Eleven bodies explicitly exclude the use of webcams for VS, whilst twelve do not address the issue (one despite an Opinion inviting it to clarify the issue). Several bodies, however, explicitly mention the use of webcams, e.g.:

- one reserves the possibility to use webcams for investigative purposes (see also above);
- at another body, one motion-activated webcam is located in the ICT Computer room, with the purpose of monitoring the room for "intrusion, climate (temperature and humidity), leaks and fire" outside office hours.

It should be noted that under Section 2.2 of the Guidelines ("**exclusions from scope**"), video-conferencing and recording and broadcasting events such as conferences, seminars, meetings, or training activities for documentary, training, or similar purposes are not covered by the Guidelines.

As noted in Section 2.2 of the Guidelines in this context, "these and other potential uses, while they may fall under the Regulation, and thus, may require appropriate data protection safeguards, are not discussed in these Guidelines. Therefore, their compliance needs must be assessed by the Bodies on a case-by-case basis". Since these uses are not discussed in the Guidelines, they are not part of this report on compliance with the Guidelines either.

5. Areas under heightened expectation of privacy

Section 6.8 of the Guidelines highlights that "Areas under heightened expectations of privacy should not be monitored. These include, typically, individual offices (including offices shared by two or more people and large, open-plan offices with cubicles), leisure areas (canteens, cafeterias, bars, kitchenettes, lunchrooms, lounge areas, waiting rooms, etc), toilet facilities, shower rooms and changing rooms.
An **impact assessment** must be carried out in case the Institution wishes to derogate from these rules. A **prior checking by the EDPS** will also be required". (emphasis added)

As has been pointed out earlier by the EDPS[28] in this respect: where bodies have no intention of operating VS equipment in areas under heightened expectations of privacy (such as in individual offices), this should be clearly confirmed in the body's VS policy.

Under Section 11.2 of the Guidelines, if any cameras are placed at a location where those present would have a heightened expectation of privacy (Section 6.8 of the Guidelines) or where the cameras would otherwise be unexpected and come as a

[28] See footnote 7.

surprise, an additional on-the-spot notice must be provided in the immediate vicinity of the monitored area (e.g. at the door of an individual office under surveillance).

Based on the information provided in the state-of-play report, several bodies monitor areas under heightened expectations of privacy. For example, one body foresees monitoring areas under heightened expectation of privacy "exceptionally, in the case of duly justified security needs" (which are not further specified) whilst audit findings include cameras in corridors and another body monitors a fitness room.

6. High-tech/intelligent or sound recording/"talking" CCTV

The Guidelines in Section 6.9 list items qualifying as **"high-tech VS tools" or "intelligent VS systems"**, which are permissible only subject to an impact assessment and prior checking. These notably include "*infra-red or near-infrared cameras, thermal imaging devices and other special-use cameras that can capture images in the dark or under low-light conditions*".

In this particular context, the EDPS is for example examining a notification by an agency, where the use of infrared cameras is foreseen ("can be used at outdoor entry/exit points if other security measures are not effective", but the notification does not refer to "high-tech VS" as reason for prior checking). However, based on the information available to the EDPS at this stage, it cannot be excluded that other notifications -preceded by an IA- will be required (e.g. where infrared detectors operate outside working hours to detect intruders or where technical specifications of the cameras include temperature sensors).

The Guidelines (Section 6.9) note that the following features in and of themselves do not require an impact assessment or prior checking:
- motion detection to limit video signals to events worthy of observation and recording,
- configuration of a motion detection system so as to send alarms to security staff when it identifies that someone accesses a restricted area (e.g. a locked IT room outside office hours),
- customary panning, tilting and limited optical and digital zooming capabilities.

On the upside, twelve bodies explicitly exclude the use of "high-tech" or intelligent CCTV.

Due to their intrusiveness, the Guidelines in Section 6.12 stipulate that, in principle, the use of **sound recording and "talking CCTV"** are prohibited, with the exception of using them as a back-up system for access control outside office hours. No body reports the use of sound recording and "talking CCTV". As already noted above, one body reported that whilst audio recording and "talking CCTV" were technically feasible with some of their camera models, these options were not actually used in practice. Nine bodies explicitly exclude sound recording / "talking" CCTV, two bodies only explicitly exclude sound recording.

7. Interconnected VS systems

Twelve bodies explicitly exclude interconnecting their VS system. The EDPS would like to note that where bodies have no intention of interconnecting VS equipment, this should be clearly confirmed in the body's VS policy.

Of the three bodies stating that they do interconnect their system, none have provided an IA so far (although one IA seems to have been initiated). The EDPS would like to highlight that according to the Guidelines (Section 6.10), the interconnection of an body's VS system with the VS system of another body or of any other third parties is **subject to an IA and a prior checking notification** and an IA is also required if a single body operates several separate systems.

8. Covert surveillance

As further outlined in Section 6.11 of the Guidelines, the use of covert surveillance should be avoided, as it is highly intrusive due to its secretive nature, has little or no preventive effect and is often merely proposed as a form of entrapment to secure evidence. Under the Guidelines, proposed exceptions must be accompanied by a compelling justification as well as **an IA and must be notified for prior checking** by the EDPS.

The EDPS welcomes that ten bodies explicitly exclude the use of covert surveillance[29], one body (CdT) at the express request of its Staff Committee. With that said, the EDPS would like to reiterate its earlier recommendation[30] that each body should verify whether it always installs the cameras and provides sufficient notice in such a way that the practice will not constitute "covert surveillance" as defined in Section 6.11. This may be the case, for example, if cameras are placed in areas under heightened expectations of privacy (such as an individual's office) without appropriate notice even if the person(s) occupying that area consented to (or requested) the placement.

- The EDPS had previously invited one institution that had announced its plans to operate covert surveillance to carry out an IA and if -based on such an impact assessment- it should chose to resort to covert surveillance, to submit its plans to the EDPS for prior checking[31]. Unfortunately, a register of covert surveillance measures seems to have been established by that institution, although no prior checking notification on this particular issue has been submitted.

- Another body notes that "Covert video surveillance (use of webcams) is authorized under special circumstances, without prior checking with the EDPS, so that investigations cannot be compromised" (also see above, Part 4).

[29] For purposes of the Guidelines, covert video-surveillance has been defined (Guidelines, Section 6.11) as "surveillance using cameras that are either intentionally hidden from view, or are otherwise installed without appropriate notice to the public, and therefore, it is reasonable to assume that the individuals monitored are unaware of their existence".
[30] See footnote 7.
[31] Ibidem .

9. Retention periods

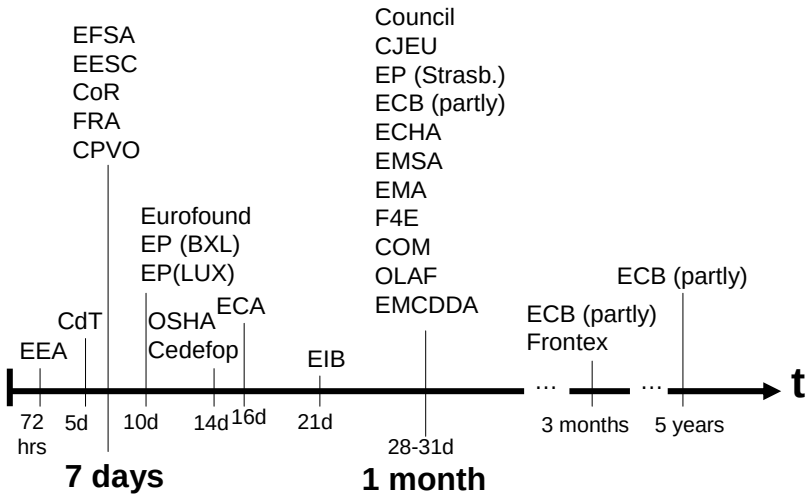
Section 7.1.1 of the Guidelines notes under "General principles" *inter alia* that it must be considered whether recording is necessary at all and whether live monitoring without recording would be sufficient. In this spirit, since a particular camera points directly to the street, one body has decided not to record from it, "respecting this way...the rights of privacy of the people passing on the street".

Under **Article 4(1)(e) of the Regulation**, recordings must not be retained longer than necessary for the specific purposes for which they were made (see also Section 7.1.1 of the Guidelines). Overall, retention periods reported by bodies **vary significantly between 72 hours and 3 months** (5 years in one, admittedly exceptional case).

Standard retention period: seven days

Under Section 7.1.2 of the Guidelines the retention period for typical security purposes cannot exceed one week. When cameras are installed for purposes of security and access control, one week should in most cases be more than sufficient for security personnel to make an informed decision whether to retain any footage for longer in order to further investigate a security incident or use it as evidence. Indeed, these decisions can usually be made in a matter of hours. Therefore, bodies should establish a retention period not exceeding seven calendar days. In most cases a shorter period should suffice.

The EDPS welcomes that seven bodies established relatively short retention periods (between three days and one week) and thus manage to (at least on average) meet the benchmark of seven days stipulated as standard retention period in the Guidelines. One body with a ten days retention period flatly notes that shortening this period by three days does not justify the additional costs for resolving the issue. Whilst the EDPS can relate to such considerations in principle, it would have preferred some fact-based argumentation, e.g. a concrete cost-estimate.



As previously clarified by the EDPS[32], unless bodies provide sufficient justification and adequate safeguards, they should reduce the retention period to seven days or less, as recommended in the Guidelines.

Justifications brought forward[33] include e.g. the value and/or confidentiality of items (e.g. business secrets) stored on the premises or very particular requirements related to nuclear facilities. One body refers to "*la pratique de malfaisants/terroristes qui effectuent un repérage des installations avant de commettre un acte*", but it remains vague in how far this assumption can be considered evidence based and/or has been the subject of discussions with local police authorities.

Certain circumstances referred to in the state-of-play reports can not be considered as *per se* suitable justifications:

- **Christmas holidays.** Two bodies adopted a retention period of 14 and 16 days respectively, referring to limited resources and, oddly, to the fact that the body "stops functioning...between Christmas and New Year". It would seem that other bodies have found technical solutions to both issues. At any rate, specificities regarding a *once-a-year* event can hardly justify a prolonged *standard* retention period.

[32] See footnote 7.
[33] In support of its 31 day retention period, one body notes that "The Security Office has put forward a number of unobjectionable arguments in support of this extended time limit..." Whilst this does not exclude that sufficient justification and adequate safeguards exist, the EDPS regrets to not be in a position to test these "unobjectionable arguments" or report on them, as they have not been provided.

- **Downtown location.** The EDPS would like to highlight that, as illustrated by the example given in Section 7.1.3 of the Guidelines[34], the fact that a body is located in a busy downtown area cannot by itself warrant an exception to the standard retention period recommended in the Guidelines. This does, of course, not exclude that a body provides in a verifiable manner proof of the existence and extent of alleged security risks[35], in particular of an increased crime rate in its vicinity, to actually justify a prolonged retention period.

- **Long reaction period by national authorities / local police**. A number of bodies note that a retention period longer than seven days is necessary to meet expectations of national authorities / local police.
    - One body (suggesting a three months retention period) notes that the currently applicable 10 days retention period is much too short where victims and national authorities only notify security incidents several months after;
    - Another body notes that one month can be considered a reasonable delay where infringements have not been indicated immediately[36];
    - A third body refers to a customary two weeks delay before incidents are reported to the security service;
    - Also a fourth body refers to delays in requests by national authorities to justify a longer retention period of generally 30 days. However, audit findings would suggest that, in reality, technical restrictions are the reason behind retaining footage longer (recorders erase variably on FIFO basis), in fact even longer than 30 days (i.e. exceeding both Guidelines and policy).

  To the EDPS it would seem that this is a matter of informing stakeholders, including national authorities and local police forces, of the constraints regarding the retention of video footage under the Regulation (as outlined by the Guidelines). If not properly informed about the fact that the Guidelines foresee a standard retention period of seven days, these stakeholders will have no reason to follow up on security incidents within a period shorter than the "customary" period that has so far been applied by the body. Where bodies want to cooperate with local police forces beyond their own mission (e.g. for the purpose of preventing bicycle thefts outside buildings), the Guidelines foresee the possibility of **coordination with Member States' authorities**.

- **Required by national legislation.** Three bodies claim that a retention period exceeding seven days is required by national law. It should be noted that national laws on data protection more frequently provide for a maximum threshold rather than imposing a necessary longer

[34] "Agency B...located in the heart of a busy downtown area with a train station nearby and heavy pedestrian traffic on the pavement of the streets outside its buildings".
[35] See Section 5.7 of the Guidelines.
[36] *"...correspond à un délai raisonnable consécutif à le commission d'une infraction qui n'a pas été signalée sur le champ...".*

retention period. In addition to this consideration, the EDPS would reiterate that, as pointed out in Section 4.4 of the Guidelines, the applicability of national data protection law, in any event, is limited by the privileges and immunity enjoyed by the bodies pursuant to Article 343 TFEU[37] and Protocol (No 36) on the privileges and immunities of the European Communities (1965)[38].

Special retention periods

In case the surveillance covers any area outside the buildings on **Member State (or third-country) territory** (typically those near entrance and exit areas) and it is not possible to avoid that passers-by or passing cars are caught on the cameras, the EDPS recommended in the Guidelines (Section 7.1.3) reducing the retention period to **48 hours** or otherwise accommodate local concerns whenever possible. Although most bodies confirm that they keep VS on Member States' territory to an "absolute minimum" (no information has been received for third countries), only one body (Council) has expressly reduced the respective retention period to 48 hours.

As mentioned in Section 7.1.4 of the Guidelines, the EDPS may recommend shorter retention periods (or **only live monitoring**) when this is necessary to minimise the intrusion into the privacy and other fundamental rights and legitimate interests of those within the range of the cameras. In this context, the EDPS welcomes that one body has taken the decision to limit surveillance to live monitoring and not to record from a camera pointing directly to a street on its host Member State's territory, "respecting this way ... the rights of privacy of the people passing on the street".

Using the example of **political protests** held in front of a body, Section 7.1.4 of the Guidelines noted that "the EDPS may recommend that, in the absence of the detection of a security incident, you delete the recordings of each peaceful protest within **2 hours** of the end of the protest at the latest (or consider live monitoring only)". One institution expressly noted its intention to erase footage of demonstrations within two hours following the protests ("*si possible dans les 2 heures suivant la fin de la manifestation*"); another institution promised to examine the technical possibilities of doing so. Regrettably, another body considers that "even if there exists an obvious risk to the privacy of the participants of a demonstration", at the same time, establishing a prolonged retention period of 28 days - including for footage of demonstrations - is fully justified based on considerations such as the location of the body (downtown), the value of the information retained there and the particularities of the premises.

Procedure for erasing footage and disposal of obsolete media

Section 7.1.1 of the Guidelines stipulates that if a body opts for recording, it must specify the period of time for which the recordings will be retained - and

[37] Treaty on the Functioning of the European Union.

[38] Official Journal C 321 E, 29/12/2006, pp. 318-324. Note that some of the so-called "headquarters agreements" concluded between the Institutions and their host countries specifically state that national data protection laws shall not apply to the Institution. This is the case, for example, with the European Central Bank.

after the lapse of this period, the recordings must be erased. No body reported on any particular procedure covering the erasure of footage, but six bodies noted that footage was erased automatically by overwriting. No body has put in place a procedure for disposing of obsolete media. This causes some concern, as at least one institution relies on VHS cassettes which will require some form of shredding after many cycles of use.

Register of recordings kept beyond retention period

The Guidelines in Section 7.2 stipulate that each body keep a register of recordings retained beyond the retention period. Only twelve bodies confirmed that they keep such a register even though the EDPS had recommended the adoption of this tool to help ensure transparency and good administration[39].

9. Access rights

17 bodies note that under their (draft) policy or according to their standard practice, access rights are limited to a small number of clearly identified individuals. 14 bodies confirm that these limited access rights were attributed on a strictly need-to-know basis and twelve bodies confirmed that ensured that authorised users can access only those personal data to which their access rights refer[40]. Eleven bodies have clearly stipulated that only the "controller" or those specifically appointed by the controller for this purpose should be able to grant, alter or annul access rights.

The EDPS welcomes that - according to the information provided in their state-of-play reports- eight bodies have achieved compliance with the requirements of the Guidelines regarding access rights to footage so far. But as already previously noted[41], further efforts are necessary to ensure that a consistent policy is established in this regard by all bodies, that the policy is implemented, and that it is effectively communicated to data subjects. The EDPS specifically emphasizes the need to implement a reliable logging system to ensure that a designated third party within the body can check at any time who accessed the system, when and which actions were performed.

10. Data protection training

As further outlined in Sections 8.2 of the Guidelines, all personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, should be given data protection training and should be familiar with the provisions of the Guidelines insofar as these are relevant to their tasks. Where VS is outsourced, Section 14.1 of the Guidelines stipulates that the contracted company must provide appropriate training to its staff, including on data protection, and that any direct or indirect subcontractor must be bound by the same obligations as the direct contractor.

Only eleven bodies reported that an initial training had taken place (with only six of them meeting the deadline of 1 January 2011). Eleven bodies foresee

[39] See footnote 7.
[40] Article 22(2)(e) of the Regulation.
[41] See footnote 7.

training when a new system is installed, when significant modifications are made to the system or for newcomers (one body doing so by providing annual training sessions). With a particular view to outsourced VS, only seven bodies clearly confirmed that external staff had been covered by training activities. The EDPS consequently urges all bodies which have not done so yet to provide all personnel with access rights, including outsourced personnel with data protection training and familiarize them with the provisions of the Guidelines insofar as these are relevant to their tasks.

Three bodies have plans to annually repeat the training exercise, the rest of the bodies opting for a two year or "at least every two years" period. One institution (EP) reported plans to outsource this future activity to a security company based on a training programme approved by its DPO.

11. Confidentiality undertakings

The Guidelines stipulate in Section 8.3 that all personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, as well as the outsourced companies themselves, should sign confidentiality undertakings to ensure that they will not transfer, show, or otherwise disclose the content of any video-surveillance footage to anyone except authorised recipients.

Twelve bodies reported that such confidentiality undertakings have been signed, but only six provided the EDPS with a template of their undertaking. Best practice examples include the undertaking provided by Eurofound as well as the undertaking provided by EEA, which contains a declaration according to which copies of the VS policy and the security policy have been received (see Annex 2).

12. Transfers & disclosures

Routine transfers. For 14 bodies, routine transfers are regulated in their VS policy and 13 bodies stipulate in their policy that the DPO will be consulted on ad hoc transfers (one body only consults "if doubts exist about the legal aspects of the transfer"). As has been previously noted by the EDPS[42], bodies need to make efforts to ensure that a consistent policy is established in this regard, but also that the policy is implemented, and that it is effectively communicated to data subjects.

Transfer to EU investigative bodies. 15 bodies foresee in their (draft) VS policy the possibility to transfer footage to EU investigative bodies (another body foresees this possibility in the absence of a formally adopted policy). Seven bodies (CJEU, EP, Frontex, CPVO, ECHA, EMCDDA, EASA) do not explicitly exclude data mining in this context as required by the Guidelines.

> As further outlined in Section 10.3 of the Guidelines, the relevant VS footage may, in exceptional cases, be transferred if this is requested by:
> - the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF;

[42] See footnote 7.

- the Commission's Investigation and Disciplinary Office ("**IDOC**") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within your Institution,
provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining should be accommodated.
Management, human resources, or other persons involved should not be provided copies or otherwise allowed access to video-surveillance footage outside the above formal procedures.

One body would seem to go beyond the limits of helping investigations or prosecutions of a *sufficiently serious disciplinary offence* by seemingly generally allowing the transfer for *all* breaches of Staff Regulations and rules. If stipulated in such generality and without further qualification, this would seem disproportionate, as an infringement of staff conduct rules cannot in all cases be compared with criminal offences.

Transfers to national authorities. As noted in Section 10.4 of the Guidelines, bodies may, in most cases, accommodate requests from national police when the recordings are necessary to investigate or prosecute criminal offences, provided that data are requested in the framework of a specific criminal investigation. However, no general requests should be accommodated for data mining purposes.

15 bodies foresee in their (draft) VS policy the possibility to transfer footage to national authorities, three seemingly limiting this to police forces. Five bodies foresee such a possibility in the absence of a formally adopted policy. Regrettably, out of those 20 bodies foreseeing such a possibility, 15 do not qualify this at all by the **requirement of a formal written request** signed by a police officer having a sufficiently high rank, or a similar formal request or a waiver of immunity if the footage concerned an EU staff member. Four bodies at least stipulate the requirement of a formal written request. One body notes that *the most frequent case* is a written request by the competent magistrate.

Under Section 10.5 of the Guidelines, **each body should keep a register** - whenever possible, in an electronic form - of transfers and disclosures, in which each transfer to a third party should be recorded. Eleven bodies provided a print-out of their (mostly: so far empty) register, three bodies reported having one. In the case of one body, the police must sign an acknowledgement of receipt if it receives footage, but it remains unclear which procedural rules (e.g. archiving) apply to these receipts afterwards.

13. On-the-spot notice

Under Section 11.2 of the Guidelines, the on-the-spot notices should include a pictogram and as much of the information listed under Article 12 of the Regulation as is reasonable under the circumstances. The notice must:
- identify the "controller" (the name of the Institution is usually sufficient),
- specify the purpose of the surveillance,
- clearly mention if the images are recorded,
- provide contact information,
- provide a **link to the on-line video-surveillance policy** (emphasis added).

If any area outside the buildings is under surveillance, this should be clearly stated. A notice in such a case merely stating that *the building* is subject to video-surveillance is misleading. The signs must be placed at such locations and be large enough that data subjects can notice them before entering the monitored zone and can read them without difficulty. This does not mean that a notice must be placed next to every single camera.
The signs within the buildings must be in the language (or languages) generally understood by staff members and most frequent visitors. Signs outside the buildings (if any areas outside are monitored) must also be posted in the local language (or languages).

19 bodies confirm that they have put in place pictogrammes; those provided in the context of the state-of-play report figure throughout this report as illustrations.

When it comes to the **content of the on-the-spot notice** required, the level of **compliance is significantly lower**: only two bodies (EEA, ECB for its construction site) meet all content requirement stipulated in the Guidelines (see above), including the link to their on-line VS policy. This limited compliance is surprising, as **Appendix 2 of the Guidelines contains a sample on-the-spot data protection notice**:

[Insert your video-surveillance pictogram: you may consider, for example, the ISO pictogram or the pictogram customarily used where you are located.]

For your safety and security, this building and its immediate vicinity is under video-surveillance. No images are recorded.
[Alternative: The recordings are retained for 48 hours.]

For further information, please consult www.*domainnameofyourinstitution*/cctv or contact the Agency's security unit at [telephone number and email address].

[Include multiple language versions when applicable.]

In only four more cases (ECB for its existing premises, CdT, EMA, ECA), the content requirements are met with the exception of the link to the VS policy. The EDPS finds regrettable that in particular big bodies with broad exposure to the general public do not comply with the clear guidance provided by the Guidelines in this respect. According to the information provided in the state-of-play reports, the EP on-the-spot notice lacks specifications as to the controller, the purpose of surveillance, the fact that images are being recorded, contact information and a link to the EP's VS practice (in the absence of an officially adopted policy) and, despite surveillance

of areas outside buildings, only states that the buildings are subject to VS ("*batiments sous vidéo-surveillance*"). The on-the-spot notices of COM, whilst identifying a controller, suffer from the same deficiencies.

Furthermore, based on the (limited) information provided in the state-of-play reports, the **EDPS is reasonably assured with regard to five bodies only** (EFSA, ECB, Eurofound, EMSA, F4E) **that existing on-the-spot notices are adequately placed**. In the absence of onsite visits so far, the EDPS trusts that where on-the-spot notices are allegedly available "adjacent to the areas under surveillance" or "at every place where cameras are present", this includes on-the-spot notices adequately placed to inform the general public of the monitoring taking place on Member States' territory (where applicable). The EDPS would like to reiterate in this context that if any area *outside the buildings* is under surveillance, this should be clearly stated, and that a notice merely stating that *the building* is subject to video-surveillance in such a case is misleading. For one body, information provided includes the audit finding that there are no on-the-spot notices on the perimeter of the building where passers-by could be inadvertently recorded. Against this background, the EDPS welcomes that at Eurofound, although the on-the-spot notices do not meet the content requirements, they are posted inter alia "on the perimeter fencing".

Regarding the **languages in which the on-the-spot notices are posted**, the EDPS again had to rely on the limited information provided in the state-of-play reports. 15 bodies claim that they comply with the Guidelines, including the use of local language versions where required.

On-the-spot notices are the primary link between most stakeholders (staff, visitors, general public) and the bodies using VS. The EDPS consequently urges all bodies as a matter of urgency to install on-the-spot notices in all locations required and to ensure that their content is in line with the requirements stipulated in the Guidelines. This notably includes a link in the on-the-spot notice for reasons of transparency and accountability, which also implies actually publishing each body's VS policy on-line (see section 14).

15 bodies claim that copies of their detailed data protection notice (VS policy) are instantly available upon request from their security staff and reception personnel. EMCDDA notes that "an information paper is available at the

entrance in case people would like to get more information", but does not specify the content of that information paper. For two bodies, audit findings include deficiencies in this respect, including that at one body "reception desk staff have not yet been notified of the procedure for providing effective and comprehensive information relating to the video protection system (existence of a policy, hand-outs, etc.)".

14. Publication of an online policy

Out of the 18 bodies having provided (draft) policy documents, *all* claimed in their policy to have published their policy or a restricted/limited version of it online. The EDPS tested access to those public policies (or on-line data protection notices) by visiting each body's webpage and using the respective search engine by searching with the terms "CCTV" and "video-surveillance". Disappointingly, only three bodies provided relevant information, one of a very limited scope (related to visitors only). Best practice examples are the EEA[43] and the CPVO, which under the search term "video surveillance" provide direct access to their online data protection notice as well as -additionally- to the EDPS Guidelines[44].

Given the transparency and accountability implications and the comparatively limited effort needed to publish a policy (or a restricted/limited version of it) online, the EDPS urges all bodies to ensure that the information is more easily available to everyone and provided in a more user-friendly format. This should include, in all cases, the publication of the body's video-surveillance policy both on the body's internet and intranet sites.

15. Individual notice and access requests by the general public

Section 11.4 of the Guidelines provides that, in principle, individuals must be given individual notice if they were identified on camera provided that one or more of the following conditions apply:
- the identity of the individual is noted in any files/records,
- the video recording is used against the individual,
- the video recording is kept beyond the regular retention period,
- the video recording is transferred outside the security unit *or*
- the identity of the individual is disclosed to anyone outside the security unit.

According to the information provided in the state-of-play reports, 14 bodies foresee such an individual notice in their (draft) policy or according to their reported standard practice, some without actually defining a procedure for this purpose. One body does not foresee any individual notice, but noted that "the

[43] See http://www.eea.europa.eu/legal/privacy/data-protection-at-a-glance.
[44] http://www.cpvo.europa.eu/main/en/home/documents-and-publications/data-protection/video-surveillance

data subject can exercise his right of rectification on the report written by security staff in connection with a security incident". This illustrates why under the conditions specified in the Guidelines, an individual must be notified if they have been identified on camera - how would any data subject otherwise learn of the existence of such a "report written by security staff in connection with a security incident"?

One body informed the EDPS that, although parts of the draft policy seem to meet this requirement, other parts of the draft policy as well as current standard practice do not, as until now, no such individual notice had ever been given in order not to compromise ongoing investigations[45]. The EDPS would like to note that no such blanket exemption from the transparency requirement should be applied on these grounds. The Guidelines are considerably more nuanced than this particular body's approach in this respect, stipulating that provisions of notice may *sometimes* be delayed *temporarily*. The Guidelines mention that this could be considered where it is *necessary* for the prevention, investigation, detection and prosecution of criminal offences or where other exceptions under Article 20 of the Regulation may apply in *exceptional* circumstances.

The EDPS welcomes that, according to the information provided in the state-of-play reports, 19 bodies address the issue of access requests by the general public in their (draft) policy or have reported on their standard practice in this respect in the absence of an officially adopted VS policy. In the context of protecting the rights of third parties, one institution notes that it is not always technically possible to single out an individual person from the footage and notes that for those cases, in order to not infringe the rights of third parties, the requesting party should turn to the EDPS[46]. In the absence of an indication as to how the EDPS can solve this body's technical problems in these cases, this would not seem the appropriate way forward. If it is not possible to safeguard the rights of third parties (including by asking and obtaining their consent), the controlling body should provide a reasoned response rejecting the access on these grounds.

Ten bodies report that they meet the requirement of offering access to the minimum information required under Article 13 of the Regulation free of charge and twelve bodies seem to have rules in place to ensure that this happens within the time-limits provided by the Guidelines.

16. Outsourcing

Section 14.1 of the Guidelines on "Outsourcing video-surveillance" notes that if the body outsources any part of its VS operations, it remains liable as a "controller" and the obligations of the processor with respect to data protection must be clarified in writing and in a legally binding manner. This usually means that there must be a written contract in place between the body and

[45] "*jusqu'à présent, il n'y a jamais eu de notification individuelle afin de ne pas compromettre les investigations*".
[46] "*Pour ne pas porter atteinte à ces autres personnes qui ne s'avéreraient pas concernées par la demande, le requérant pourra s'adresser à l'EDPS pour faire contrôler la licéité des données*".

the service provider. The latter must also have a written contract with its subcontractors.

Eight bodies outsourcing VS provided the EDPS with the written contract (or excerpts of it) concluded with the security service provider, four additionally provided a contract concluded between that company and a subcontractor. Only one body (EFSA) provided contractual documentation meeting all content requirements outlined in the Guidelines (pp. 50/51).

17. Security measures

For obvious reasons of confidentiality, **this Report does not mention any details** on the evaluations of security risks (insofar as these were at all provided) or provide comments on any particular security measures put in place by bodies. However, on some selected issues, the EDPS would like to comment as follows:

- Under the Guidelines, the location of monitors must be chosen so that unauthorised personnel cannot view them. If they must be near the reception area, the monitors must be positioned so that only the security personnel can view them. Where visitors can see the pictures of the cameras when standing at the reception desk or when leaving the building and "due to structural reasons, it is not possible to relocate the monitors", the possibility of encapsulating of framing those monitors should be examined.
- A reliable digital logging system must be in place to ensure that an audit can determine at any time who accessed the system, where and when. The logging system must be able to identify who viewed, deleted, copied or altered any video-surveillance footage. In this respect, and elsewhere, particular attention must be paid to the key functions and powers of the system administrators, and the need to balance these with adequate monitoring and safeguards.
- A process must also be in place to appropriately respond to any inadvertent disclosure of personal information. This should include, whenever possible, notification of the breach to those whose data are inadvertently disclosed as well as to the body's DPO.
- The security analysis as well as the measures taken to protect the video-surveillance footage must be adequately documented and must be made available for review to the EDPS upon request.
- Finally, the body must act with due diligence in its choice and supervision of its own and security provider's staff.

Part 4: Where do we go from here?

Prior checking

It should be noted that in all cases where prior checking is necessary, **bodies must first carry out an impact assessment and submit their notification prior to the start of processing operation**. Such prior checks may result in a "joint" approach on particular topics and can include on-the-spot fact-finding.

Inspections

The EDPS may also carry out thematic on-site inspections at selected bodies focusing on VS. The time period and schedule for these inspections remains to be established in the light of the findings of this Report.

Inter-institutional cooperation

There seems to be untapped potential in the exchange of best practices amongst bodies (e.g. on technical solutions for similar security issues), giving advice to newly established bodies (e.g. on implementing a "privacy by design" approach) and the option to undertake peer-reviews in the context of follow-up audits. The EDPS stands ready to facilitate such cooperation.

Cooperation with national data protection authorities (DPAs)

Section 4.4 of the Guidelines notes that the DPA of the Member State in which the body is located may have an interest with respect to monitoring that takes place outside the buildings. As noted in Part 3, Section 3 above, ten bodies have already consulted the relevant DPA(s); regrettably, the state-of-play reports submitted did not provide details as to the recommendations made by these national DPAs. There are, however, indications of remaining issues that will need to be resolved in close cooperation with national DPAs.

Annex 1: List of institutional acronyms[47]

CdT	Centre de Traduction
Cedefop	European Centre for the Development of Vocational Training
CFCA	Community Fisheries Control Agency
CoR	Committee of the Regions
Council	Council of the European Union
CJEU	Court of Justice of the European Union
COM	European Commission
CPVO	Community Plant Variety Office
EACEA	Education, Audiovisual and Culture Executive Agency
EACI	Executive Agency for Competitiveness & Innovation
EAHC	Executive Agency for Health and Consumers
EASA	European Aviation Safety Agency
ECA	European Court of Auditors
ECB	European Central Bank
ECDC	European Centre for Disease Prevention and Control
ECHA	European Chemicals Agency
EDPS	European Data Protection Supervisor
EEA	European Environment Agency
EESC	European Economic and Social Committee
EFSA	European Food Safety Authority
EIB	European Investment Bank
EIF	European Investment Fund
EIT	European Institute of Innovation and Technology
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMA	European Medicines Agency
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EP	European Parliament
ERA	European Railway Agency
ERCEA	European Research Council Executive Agency
ETF	European Training Foundation
Eurofound	European Foundation for the Improvement of Living and Working Conditions
F4E	Fusion for Energy
FRA	European Union Agency for Fundamental Rights
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GSA	European Global Navigation Satellite Systems Agency
OHIM/OAMI	Office of Harmonization for the Internal Market
OLAF	European Anti-fraud Office
Ombudsman	European Ombudsman
OSHA	European Agency for Safety and Health at Work
REA	Research Executive Agency
Sesar	Single European Sky ATM Research Joint Undertaking
TEN-T EA	Trans-European Transport Network Executive Agency

[47] See http://europa.eu/agencies/regulatory_agencies_bodies/policy_agencies/index_en.htm and http://europa.eu/agencies/executive_agencies/index_en.htm.

Annex 2: Best practice example confidentiality undertaking

EUROPEAN ENVIRONMENT AGENCY

PERSONAL DATA PROTECTION
CONFIDENTIALITY UNDERTAKING

I (insert full name)

Position/Title _____

1. undertake to not transfer, show or otherwise disclose the content of any video-surveillance footage to anyone except authorised recipients as listed in the EEA Security policy for video-surveillance*;
2. confirm that I have received a copy of the EEA Video-surveillance policy and the EEA Security policy for video-surveillance

Signed:	Dated

_____

* The EEA Video-surveillance policy and Security policy on video-surveillance adopted by the EEA Executive Director on XX/YY/ZZZZ were prepared in line with the Guidelines produced by the European Data Protection Supervisor in March 2010, see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-0317_Video-surveillance_Guidelines_EN.pdf.