Last updated on 17 March 2010

Frequently asked questions on video-surveillance: prior checking

1. What is prior checking? Article 27 of the Data Protection Regulation[1] provides that "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope, or their purposes shall be subject to prior checking by the European Data Protection Supervisor". The purpose of prior checking is to ensure that certain systems presenting large inherent risks can only be deployed if reviewed in advance by the EDPS. This allows the EDPS to check whether the deployment of the system is justified in the first place, and if so, whether the data protection safeguards proposed by the institution are adequate and sufficient. The EDPS may also recommend additional safeguards.

2. What are the risks of video-surveillance? Video-surveillance, by its nature, has a strong capacity to be privacy invasive. Video-surveillance systems are also becoming ubiquitous and more and more sophisticated and powerful:

- Modern systems capture and record digital images that are easily copied and distributed.
- The images can be instantaneously broadcast to a multitude of recipients or posted on the Internet with the help of increasingly powerful digital communication networks.
- The digital records holding continuous, detailed information may also be conveniently stored, searched and indexed for infinite replay and analysis.
- The likelihood of images being retained for further data mining is increasing due to its technical feasibility.
- Intelligent and interconnected systems are increasingly able to match images against a database of images or track moving targets (objects or persons) in large areas.
- They are also getting increasingly good at automatically identifying pre-defined, “suspicious” behaviour. Indeed, there are areas where today or in the near future automated, dynamic-preventive surveillance is about to replace conventional static surveillance. Surveillance specialists in digital imaging research centres around the world are continuously working on making video-surveillance more and more intelligent with the aim of achieving improved efficiency by automation.
- The cameras themselves are also becoming more powerful and more

[1] 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.

sophisticated. Pan-tilt-and-zoom ("**PTZ**") cameras can pan and zoom-in on their targets from further and further away. Infra-red cameras, heat recognition devices and other special-use cameras can now capture images in the dark, see through walls and search under our clothing.

These and other new features of video-surveillance, along with the increasing ubiquity of the technology itself, pose significant risks:

- First, they offer ever-increasing and very real opportunities for both security breaches and misuse: the recordings may fall into the wrong hands or may be used by the lawful recipients for unlawful purposes.
- If the recordings are retained for a long period of time or sent to a multitude of recipients, there is an increased risk of "mission creep", that is, an increased opportunity that the images may be used for purposes not initially foreseen and specified.
- Further, the risks of video-surveillance go beyond the instances when actual abuse or misuse happens. Being watched changes the way we behave. When watched, most of us censor our speech and our behaviour. In case of widespread or continuous surveillance knowing that our every move and gesture is monitored by the cameras may have a deep psychological impact as we will feel under pressure to constantly adjust our behaviour to the expectations of those who are watching us.
- Finally, video-surveillance also has its social costs. It may not only deter criminal activities but also other legitimate forms of behaviour. This is an especially relevant concern in the workplace where people should have a reasonable expectation of privacy. Video-surveillance may also have chilling effect on political protests and demonstrations held in the vicinity of the buildings of the institutions and on other forms of protected speech.

3. Do these risks justify that the EDPS prior check every video-surveillance system? No, while the risks of video-surveillance justify that institutions take data protection seriously and adopt a comprehensive set of data protection safeguards, the EDPS does not consider it necessary to review individually every standard video-surveillance system operated by or on behalf of every institution.

The Guidelines set forth a comprehensive set of data protection safeguards for standard video-surveillance systems established for typical security purposes. To address and minimise the risks of video-surveillance, for these standard systems it is sufficient if such a video-surveillance system is

- designed after careful consideration of its data protection impacts and
- adoption of a comprehensive set of data protection safeguards as recommended in the Guidelines, including also the adoption of a video-surveillance policy and carrying out periodic audits to verify compliance with the Regulation and the Guidelines.

Some video-surveillance systems, however, remain subject to prior-checking. The purpose of this more in-depth review is to assist the institution with additional and tailor-made recommendations beyond those already set forth in the Guidelines.

4. Which video-surveillance systems are subject to prior checking? Section 4.3 of the Guidelines describes what systems are subject to prior checking. It also provides a non-exhaustive list of these: video-surveillance proposed for investigative purposes, employee monitoring, processing of special categories of data, monitoring areas under heightened expectations of privacy, high-tech and/or intelligent video-surveillance, interconnected systems, covert surveillance, sound-recording and "talking CCTV"[2].

5. Will the prior checking be comprehensive and cover all aspects of a video-surveillance system? No, in most cases the EDPS will not comprehensively review and comment on all aspects of the institution's video-surveillance practices. Instead, the EDPS will usually focus only on those aspects of video-surveillance which differ from, or are in addition to, the common practices and standard safeguards set forth in the Guidelines.

However, in some cases, the EDPS may, at his own initiative, nevertheless carry out a more comprehensive review. This may be the case, for example,

- if it is difficult to assess individual aspects of the video-surveillance system without the entirety of the system, especially if the system is complex or if a large number of exceptions, or very significant exceptions are proposed from the standard practices and recommendations set forth in the Guidelines, or
- if reasonable doubts arise regarding compliance of the remaining aspects of the system.

6. Do we need to notify the EDPS about our compliance status when we install a new video-surveillance system even if the system is not subject to prior checking? This is only necessary as a transitory measure, following the issue of the EDPS Video-surveillance Guidelines, as described in Section 15 of the Guidelines. Once you have brought your practices into compliance with the Guidelines by the end of the transitory period and notified the EDPS of your

[2] Some video-surveillance practices may also fall under one of the “specific risk” categories listed under Article 27(2): Some employee monitoring may involve performance evaluation, and thus, may require prior checking also under Article 27(2)(b). Further, video-surveillance for investigatory purposes is likely to concern personal data related to suspected offences, and thus, may also require prior checking under Article 27(2)(a).

compliance status, there will not be a need for further notifications if you upgrade your system or install a new system (unless a prior checking will be necessary).

7. When do we need to submit a prior checking notification to the EDPS and how long does it take for the EDPS to issue his Opinion? The EDPS has two months to issue his prior checking opinion, which, in case the complexity of the case requires, may be extended by an additional two months. These timelines are suspended if the EDPS requests further information from you[3]. When a system is subject to prior checking, you cannot start using the new video-surveillance system before the EDPS has issued his Opinion and you have followed-up and addressed his concerns[4].

Considering these timelines, you should aim at submitting your prior checking notification to the EDPS (via your data protection officer) well in time *before you wish to start operating the new system*. However, whenever possible, it is advisable to send your notification even earlier, *before you make any financial commitments to your new system.* This is especially recommended if doubts arise regarding the data protection aspects of your planned system during the initial assessment and consultation process or if your system is particularly complex. Such an early notification may ensure that you do not incur financial losses in case the EDPS requires major changes to your system (for example, if he concludes that some cameras should not be used at all or their specifications or locations need to be changed).

Based on the foregoing, the EDPS recommends that you allow at least four months for the EDPS to process your notification before the proposed launch date (or commitment to purchase). More, if you expect lengthy exchanges, meetings, and on-the-spot checks in the framework of prior checking a complex or controversial proposal.

8. What else do I need to do during the prior checking procedure? Once you have submitted your notification via your DPO, you should also

- be available to submit any additional information that may be requested by the EDPS in a timely manner,
- be ready for a meeting or an eventual on-the-spot visit or inspection and
- be available to comment on the final draft of the Opinion.

---

[3] See Regulation, Article 27(4).

[4] This is apart from the case of ex-post prior checking. Please also note that if you wish to conduct a pilot to test the system for a limited period of time and with limited coverage, the EDPS may be able to issue a provisional authorization for you for the duration of the pilot, subject to adequate provisional safeguards. Please check the modalities of this with your DPO.

9. Will the Opinion of the EDPS be made public? The EDPS prior checking Opinion is a public document. Currently, all prior checking Opinions are published on the EDPS website. Certain confidential data, including the security measures you took to safeguard your video-surveillance system may be omitted from the published version of the Opinion.