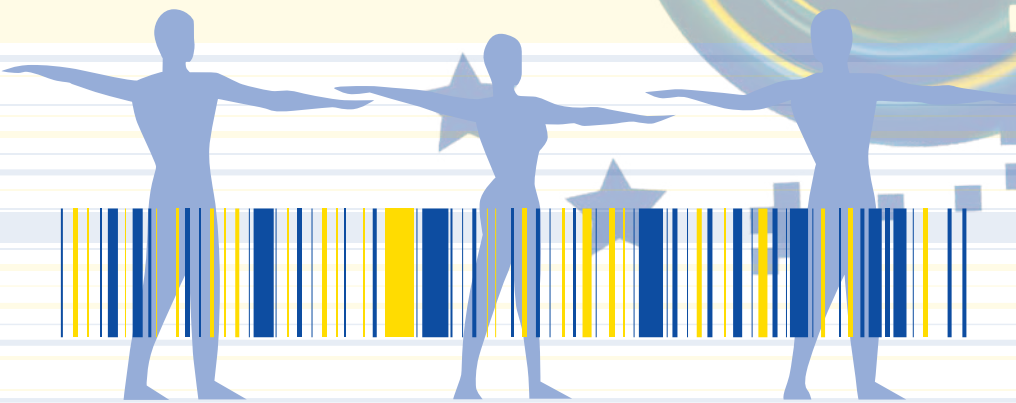
European Data Protection Supervisor

The EDPS: Keeping an eye on video-surveillance in the EU administration

EDPS factsheet 4



www.edps.europa.eu

Almost all EU institutions and bodies have **video-surveillance** in operation on their premises. The types of systems in place are as varied as the different responsibilities within the **EU administration** itself: from small executive agencies with only a few cameras (CCTV), to EU institutions and bodies with seats in a number of Member States operating several hundreds of cameras.

How does video-surveillance affect you?

Video-surveillance footage often contains images of people. Any information, such as names, dates of birth, photographs, video footage, email addresses, telephone numbers and so on that can be used directly or indirectly - i.e. combined with other pieces of information - to identify you is known as personal data or personal information.

When well designed and selectively used, video-surveillance systems are powerful tools for tackling security issues.

When the EU administration uses video-surveillance, the fundamental rights of both staff and visitors - such as the right to privacy in the workplace, free speech, freedom from discrimination (for instance if profiling is used) and the right of assembly - are affected.

The EDPS believes that if used in a selective and proportionate way, video-surveillance systems can meet security needs while also respecting your privacy.

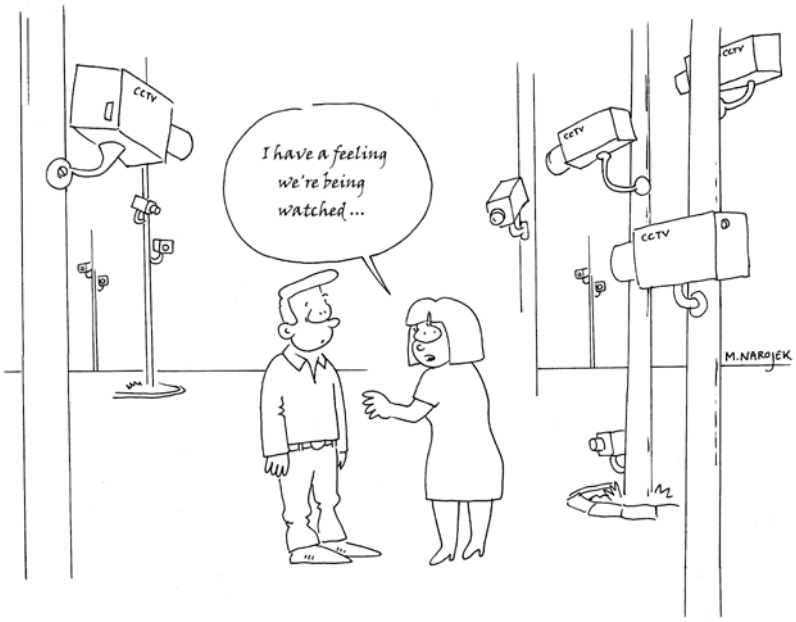
What is the role of the EDPS?

Everyone is entitled to protect their personal information. Data protection is a fundamental right, protected by European law and enshrined in **Article 8** of the **Charter of Fundamental Rights of the European Union**.

More specifically, the rules for data protection when the EU institutions and bodies process personal data are set out in **Regulation (EC) No. 45/2001**.

The EDPS is the European Union's **independent** data protection authority.

- We **monitor** and ensure the **protection of personal data and privacy** when EU institutions and bodies process the personal information of individuals;
- we **advise** EU institutions and bodies on all matters relating to the **processing** of **personal information**;



- we are **consulted** by the EU legislator on proposals for legislation and new policy development;
- we **monitor** new technology that may affect the protection of personal information;
- we **intervene** before the Court of Justice of the EU to provide expert advice on interpreting data protection law;
- we also **cooperate** with national supervisory authorities and other supervisory bodies to improve **consistency** in protecting personal information; and
- in our supervisory role, we **monitor and ensure** that the EU institutions **comply** with data protection rules; we hold the EU administration **accountable** for this compliance and promote a 'data protection culture' within the institutions.

We believe that fundamental rights and security in the use of video surveillance do not have to be mutually exclusive. Instead, **security needs should be balanced against your fundamental rights**.

How does the EDPS promote good practice in the use of video-surveillance?

- **Providing guidance to the EU administration - and beyond**

The EDPS Video-Surveillance Guidelines: The purpose of our Guidelines is to offer practical guidance to the EU administration on how to comply with the law and use video-surveillance responsibly.

Our Guidelines provide **recommendations** to the EU administration on how to design and operate their video-surveillance systems with effective safeguards in place. In setting out the principles for evaluating the need for its use, they offer guidance on how to conduct video-surveillance in a way which minimises the impact on your privacy and other fundamental rights.

- **Promoting accountability**

EU institutions and bodies are obliged to **comply** with our Guidelines and to **demonstrate** this compliance. As a supervisory authority, we ensure that they do.

While EU institutions and bodies are **accountable** for complying with data protection law, each has a degree of discretion on how to design its own system within the boundaries of this law. Our Guidelines promote practices that help balance their security needs with your privacy rights. These include putting data protection safeguards in place such as:

- the timely and automatic deletion of footage;
- developing a **video-surveillance policy** that outlines these safeguards; and
- periodic audits - both internal and by the EDPS - to ensure that the policy remains adequate and is followed.

In cases where the risks to your fundamental rights are high, the institution concerned is obliged to assess the implications of that surveillance on privacy and data protection (also known as an impact assessment).This impact assessment must then be submitted to the EDPS for **prior checking** i.e. before the surveillance becomes operational. To guide the EU administration in this area, we have published some **Frequently Asked Questions** on when to submit video-surveillance for prior checking on our website.

- **Follow-up to EDPS Guidance - raising awareness**

In February 2012, we published a **Follow-up Report** to our Guidelines. This report contained an analysis of the reports we had received from over forty EU institutions and bodies on their video-surveillance practices. As well as highlighting **best practices**, our report pinpointed where EU institutions and bodies were lagging behind in their efforts to ensure compliance with our Guidelines.

- **Monitoring compliance**

In November 2012, we reported on the findings of some **inspections** we had carried out in June and July 2012 on the premises of thirteen Brussels-based EU institutions and bodies. These inspections were one of the measures we announced in the February 2012 Follow-up Report.

The inspection report, which is not public, contains recommendations for EU institutions and bodies on how to better **inform you and the general public about video-surveillance** including:

– the existence, location and content of an **on-the-spot notice,** for instance, with a pictogramme and some basic written information, highlighting that the area is under surveillance;

– the availability and the content of a more comprehensive **data protection notice** briefly summarising why and how video-surveillance is taking place, what the safeguards are and how individuals can exercise their rights;

– the availability and the content of an **online policy** on video-surveillance detailing the broader approach of the EU institution or body concerned.

Glossary

- **Personal information or data**: Any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, e-mail addresses and telephone numbers. Other details such as health data, data used for evaluation purposes and traffic data on the use of telephone, email or internet are also considered personal data.
- **Privacy:** The right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).
- **Video-surveillance**: The 2010 EDPS Guidelines on video-surveillance define video-surveillance as the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring.
- **CCTV systems**: Closed Circuit Television systems comprising of a set of cameras monitoring a specific protected area, with additional equipment used for transferring, viewing and/or storing and further processing the CCTV footage.
- **EU institutions and bodies / EU administration**: All institutions, bodies, offices or agencies operating for the European Union (e.g. European Commission, European Parliament, Council of the European Union, European Central Bank, specialised and decentralised EU agencies).
- **Accountability**: Under the accountability principle, EU institutions and bodies put in place all those internal mechanisms and control systems that are required to *ensure compliance* with their data protection obligations and be able to *demonstrate* this compliance to supervisory authorities such as the EDPS.

Further reading:

- 2010 **EDPS Video-surveillance Guidelines**
- **Follow-up Report** (February 2012)
- **Press Release** on the EDPS report on the findings of **inspections** carried out between 15 June and 18 July 2012 on the premises of thirteen Brussels-based EU institutions and bodies
- **Frequently Asked Questions** on video-surveillance and prior checking
- 2009 **Consultation** on the EDPS video-surveillance guidelines
- **Article 47(1)(a) of Regulation (EC) 45/2001:** Powers conferred on The European Data Protection Supervisor
- 2010 **EDPS policy paper** *Monitoring and Ensuring Compliance with Regulation (EC) 45/2001*.

All EDPS documents listed in this section are available on the EDPS website: www.edps.europa.eu

@EU_EDPS

QT3012769ENC
doi 10.2804/47701

ISBN 978-92-95076-60-0

Publications Office