European Data Protection Supervisor

EDPS Newsletter

No 39 | October 2013

French and German versions will be online soon

IN THIS ISSUE

HIGHLIGHTS

LIBE Committee Inquiry on the electronic mass surveillance of EU citizens

"The three most striking points that we know at this stage are (i) the scale of the monitoring that has been going on, (ii) the number of private actors, including well known internet giants, that have apparently been involved, either actively or passively, and (iii) the development of weaknesses and backdoors in encryption, with far reaching perverse effects and very great damage to the public trust."

Peter Hustinx at the Public Hearing in Strasbourg, 7 October 2013.

EDPS hearing submission (pdf)

Smart borders: key proposal is costly, unproven and intrusive

There is **no clear evidence** that the Commission Proposals to create a **smart border** system for the external borders of the EU will fulfil the aims that it has set out, says the European Data Protection Supervisor (EDPS). Following the publication of our opinion on 18 July 2013, which focuses specifically on the **Entry/Exit System**, the EDPS said that one of the stated aims of the proposals was to replace the existing 'slow and unreliable' system but the Commission's own assessments do not indicate that the alternative will be sufficiently efficient to **justify** the **expense** and **intrusions into privacy**.

"Improving the management of border controls is a legitimate exercise. But it would be more effective to do this once a clear European policy on the management of over stayers has been established. In the absence of such a policy, the creation of yet another large-scale IT database to store massive amounts of personal information is a disproportionate response to a problem that other recently created systems may be able to help solve. It would be prudent both economically and practically to evaluate the existing systems at least to ensure consistency and best practice."

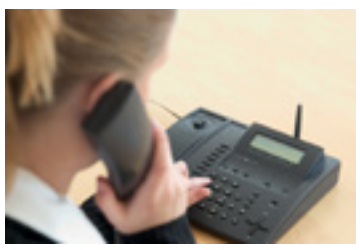
Peter Hustinx, EDPS

EDPS Opinion

EDPS press release

SUPERVISION

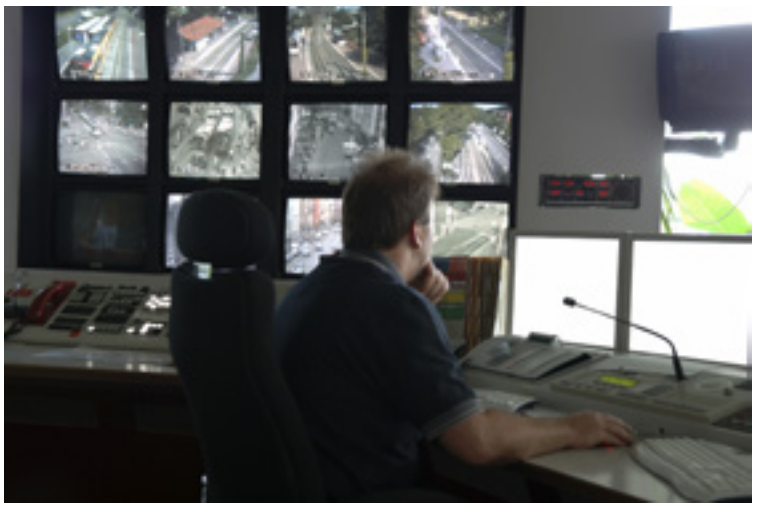
EIB: recording switchboard and security room phone conversations



The European Investment Bank (EIB) would like to occasionally record calls to and from its switchboard for security reasons and notified us of its policy on the subject. Our prior check Opinion of 20 June 2013 on the recording of these calls, included recommendations on the establishment of a clearer legal basis, a reduction of the conservation period and improving the information provided to both callers and staff working on the switchboard.

EDPS prior check Opinion

European Investment Bank



CCTV: EFSA should be vigilant over purpose limitation and scope

The EDPS 2010 Video-surveillance Guidelines mention the obligation for EU institutions to notify the EDPS if their CCTV systems involve privacy invasive high-tech installations. As the European Food Safety Agency (EFSA) uses infra-red technology in their CCTV system, they notified their video-surveillance policy to us. In accordance with these Guidelines, our Opinion referred only to those EFSA practices that do not seem to be in conformity with the Guidelines - a 'mini' prior check. Our main recommendation was the need for a data protection impact assessment for the use of the infra-red technology. We also took the opportunity to highlight other aspects of their video-surveillance policy to EFSA including the need to clarify the scope of the premises covered by the CCTV system, to keep video surveillance within the purpose limitation defined by EFSA i.e. security purposes and to inform the general public about its video-surveillance policy.

EDPS Opinion

EDPS inspects EU institutions in Luxembourg over CCTV

The EDPS Follow-up Report of February 2012 on the status of compliance of EU institutions and bodies with our 2010 video surveillance Guidelines outlined several follow-up measures, including thematic inspections. Between June and July 2012, we inspected the premises of thirteen Brussels-based EU institutions and bodies. On 9 and 10 July 2013, we carried out similar inspections of the premises of four Luxembourg based EU institutions and bodies.

As in the earlier 2012 exercise, our focus was on how Luxembourg based EU institutions and bodies inform the general public about video surveillance including:

- the placing, location and content of an on-the-spot notice (a pictogramme together with some basic written information) highlighting that the area is under surveillance;
- a comprehensive data protection notice summarising the why and how of the video surveillance;
- an outline of the safeguards and how individuals can exercise their rights;
- an online policy on video surveillance detailing the approach of the EU institution or body concerned.

The results of these inspections at the EU institutions and bodies are currently being examined.

Checking Security & Trustworthiness at the JRC

In line with EDPS recommendations following an inspection at the Joint Research Centre (JRC) in Ispra in late 2010, the JRC decided to replace its security screening procedure; it would no longer be linked to their recruitment procedures but to the access of individuals to nuclear and related sensitive areas. There would, therefore, be a need to ascertain and confirm the trustworthiness of people requiring unescorted access to JRC Ispra nuclear and related sensitive areas.

In our Opinion of 19 June 2013, on the Security Trustworthiness Check of JRC processing operations, we recognised the obligations of the JRC Ispra site to implement the recommendations of the International Atomic Energy Agency and of the Physical protection plan approved by the Italian Ministry of Industry decree. We insisted that the JRC complete this legal obligation with the new Commission Decision on security and an updated Memorandum of Understanding between the Commission security services and the JRC Ispra. Furthermore, we recommended the review of the retention period of data already collected in light of the new processing operation and to ensure that information be corrected and provided to the different individuals concerned.

EDPS Opinion

Public access requests at the ECB - balancing the interests of staff and the public

On 20 September 2013, the EDPS replied to a consultation from the European Central Bank (ECB) about public access to a register set up as part of the ethical framework rules of the ECB on the gifts received by ECB staff members.

Taking into account the ECB decision on public access and the facts of the case, our analysis took into account the Bavarian Lager judgment of the Court of Justice of the European Union and the EDPS Paper on *Public access to documents containing personal data after the Bavarian Lager ruling* and considered the public access request as a transfer that must be compliant with the Regulation 45/2001. The ECB must balance the interests of the recipient to establish the necessity of the transfer of information and that of the institution to establish if there is reason to assume that an individual's legitimate interests might be prejudiced by allowing access to his personal information.

The balance of interests should also take into account the categories of staff concerned as transparency requirements may justify the publication of the personal information of executive members or senior management members.

We concluded that the ECB should assess the possible public nature of the gift register and make it clear to the persons mentioned in the register the extent to which the processing might be publicly disclosed. Consequently, an individual would need to be informed before his personal data is disclosed for the first time and should have the right to object to the disclosure on compelling legitimate grounds pursuant to the EU data protection Regulation.

EDPS reply

EUROPEAN CENTRAL BANK

CONSULTATION

EDPS finds major deficiencies in anti-money laundering proposals

The Commission proposals for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds need to do more than make mere references to data protection.

In our Opinion of 4 July 2013 we acknowledged the legitimacy of achieving transparency of payments sources, funds deposits and transfers in order to fight terrorism and money laundering but insisted that data protection requirements should be included in legislations transposing international standards at EU level.

We were pleased to note that data protection concerns were raised by many and appeared in the impact assessment carried out by the Commission. We regret, however, that both the proposed Directive and Regulation did not fully address these concerns and did not clarify the application of EU data protection rules to the specific processing activities involved. In the proposed texts no substantial provision address data protection issues.

More specifically, we expressed concerns on the large amounts of personal information that is collected in the name of anti-money laundering and anti-terrorist purposes, in particular by professionals carrying out customer due diligence. We recommended that the purpose limitation principle be strictly respected and that further guidance be given to professionals on the data that they should or should not collect. We also highlighted that the texts should further develop the role of the rights of individuals and in particular, raise the awareness of professionals and customers. We also advised that limiting the rights of individuals is justified only if it is proved necessary.

Considering the repeated, mass and structural transfer of personal data that will take place in the framework of the proposed Directive and Regulation, we highlighted the risks linked to such transfers to third countries and advised the inclusion of dedicated substantive provisions on the transfers of personal data, such as a proportionality test, to ensure proper protection of individuals when their information is transferred.

In addition we pointed out that the data retention periods chosen need to be justified. We also insisted that the publication of sanctions imposed on professionals that do not respect their obligations under these texts, need to comply with the proportionality principle.

EDPS Opinion

EDPS press release

On the road to safety: data protection safeguards need to be applied

On 13 June 2013, the EDPS published formal comments on two draft Commission regulations in the field of intelligent transport systems which were under scrutiny by the European Parliament and the Council. The draft instruments concern the collection and provision of information for road safety information services, one for general traffic information, the other on parking possibilities for trucks. We were pleased that we had been consulted during the drafting process and that data protection elements were taken into account in the Commission drafts. Road traffic information systems in the future are likely to rely more heavily on information collected via the multitude of mobile devices that will be installed in cars or carried by their drivers, such as location aware mobile phones, connected GPS navigation systems and other intelligent transport systems, such as cameras with the capability of number plate recognition. We stressed the importance of data protection when much of the collected traffic data is related to identified or identifiable persons. We appreciate that these considerations are taken into account in the regulations, but explained that safeguards such as anonymisation of data becomes more difficult as more precise data is collected (a *study* on location data found that individuals can be identified from a very limited number of data points about their location, without any other information). The combination of data in traffic information systems, including the re-use of public sector information (Open Data) must, therefore, always be implemented with the appropriate data protection safeguards.

EDPS Comments

OFFICE FOR HARMONIZATION IN THE INTERNAL MARKET
(TRADE MARKS AND DESIGNS)

A sign of the times: data protection should be integral in the protection of trade marks

The importance of *trade marks* is widely recognised and they are protected by EU law. A trade mark is a sign (distinctive features such as words, logos, devices and so on) which serves to distinguish the goods and services of one organisation from those of another. Trade marks influence consumer decisions every day and so registration of a trade mark is one of the strongest ways to defend a brand.

On 11 July 2013, the EDPS issued an Opinion on the Commission proposals for a Directive to approximate the laws of the Member States relating to trade marks and a Regulation amending the Community trade mark regulation.

In our Opinion we stressed that the collection and processing of personal data by the central industrial property offices in the Member States and the European trade mark Agency (OHIM) must comply with the applicable data protection law. We also recommended that the modalities for the exchanges of information through common or connected trade mark databases and portals be clearly established, in particular by determining the authorised recipients of personal data, the types of data, the purpose of such exchanges and the length of the retention of the data in those IT systems. Furthermore, we recommended that if the exchanges of information between OHIM and national offices include personal data then this, as well as the types, should be clarified.

EDPS Opinion

Financial services: EU data protection rules should be taken into account

The Commission proposal for a Directive on the comparability of fees relates to payment accounts, payment account switching and access to payment accounts with basic features.

The measures on comparability of payment account fees allow consumers to have a complete overview of the offers on the market and the measures on switching make it easy for them to change their account if a better offer is available. All these elements aim to reinforce competition in the financial services market to the benefit of consumers. However, to guarantee that as many consumers as possible can really enjoy the benefits of these improvements, it is essential to ensure that every EU citizen has the right of access to basic payment account services.

In our formal comments of 27 June 2013 on this proposal, we were pleased that any exchange of personal data of the consumer by the payment service providers in the 'switching phase' is subject to the prior written and explicit consent of the consumer. We also welcomed that the proposed Directive specifically recalls the principle of necessity in the information sharing among payment service providers. However, we stressed that the proposal should mention that relevant EU data protection legislation remains fully applicable in relation to the obligations introduced by the Directive.

EDPS Comments

Sale of Counterfeit Goods via the Internet

On 18 April 2013, the Commission published a report on the functioning of the memorandum of understanding (MoU) on the sale of counterfeit goods via the internet. The report provides a detailed assessment of best practices and practical measures that successfully prevent the sale of counterfeits online, thus protecting consumers looking for genuine products in the digital internal market. The MoU was drawn up following *dialogue* between companies and trade associations covering 39 different internet sites including leading e-commerce platforms (such as eBay, Amazon, Allegro and Rakuten/PriceMinister). In our formal comments of 11 July 2013, we welcomed the publication of this report which provides information on how internet platforms participating in the MoU have implemented notice and take down procedures and on the mechanisms they have set up for cooperating and sharing information - including the personal information of alleged infringers - with rights owners. We noted the Commission's role in recognising the importance of these issues and facilitating dialogue between companies and trade associations to ensure that any measures deployed are compliant with applicable law and that they fully respect the rights of individuals to privacy and data protection. We also expressed a wish to be involved in the on-going dialogue.

EDPS Comments

Preparing for an audio visual world: a large measure of data protection must be added to the mix

On 24 April 2013, the Commission published a *Green Paper* entitled *Preparing for a Fully Converged Audio visual World: Growth, Creation and Values*. The Green Paper launches a public consultation on the implications of the on-going transformation of the audio visual media landscape: audio-visual media services are no longer only provided by traditional means and by traditional broadcasters but are also delivered by providers on demand via the internet and reach consumers through connected (often called 'smart') TVs, PCs, laptops or tablets and mobile devices such as smartphones.

In our comments of 30 August 2013, we stressed that these new modes of distribution and consumption of audio visual works generate new forms of collection and processing of users' personal information. However, it may not always be clear for users that their consumption of audio visual works and interaction with associated services leads to the processing of personal data at different levels of the provision of the services (for instance, by their device, by their ISP and/or broadcaster) nor to what extent such processing takes place, in such a way that users are not in control of their information.

We believe that any policy choice in that area should be fully compliant with the EU data protection legal framework. Among other things, we highlighted that full transparency must be ensured to users on the types of personal data collected about them and by whom, consent of the user to the processing of their data should be sought where relevant and specific attention should be paid to the protection of the privacy and personal data of children, especially in the field of advertising. Technical tools should help protect children's privacy and personal data, notably with regard to the configuration of the service and of the user's terminal.

EDPS Comments

COURT MATTERS

Court case: European Commission v Hungary

At a hearing before the Court of Justice of the European Union on 15 October 2013, the EDPS pleaded in support of the European Commission in the case Commission v Hungary (case C-288/12).

On 1 January 2012, a new constitution came into force in Hungary. Under this constitution, a new data protection authority was created and the mandate of the head of the existing authority was terminated. The EDPS pleaded that Hungary had failed to ensure that the national data protection authority was able to act with complete independence as obliged under Article 28 of Directive 95/46/EC. The EDPS argued that the mandate of the head of the authority must be protected from being terminated before the term ends without adequate justification and appropriate procedural safeguards. Adequate provisions for the transition should have been provided and a change in the legislation cannot, in itself, justify early termination.

The Opinion of Advocate General Wathelet is expected on 10 December.

This is the third case before the Court dealing with the independence of national data protection authorities. Read our previous newsletter reports on Commission v Germany (*pdf*) and Commission v Austria (*pdf*).

EDPS pleading notes

Court Case: Data Retention

On 9 July 2013, the EDPS made oral submissions at the hearing before the Grand Chamber of the Court of Justice in joint preliminary references C-293/12 and C-594/12 Digital Rights Ireland and Others. Both cases concern the validity of the Data Retention Directive 2006/24/EC. It was the first time that the Court decided, on the basis of Article 24 of its Statute, to invite the EDPS to attend a hearing (in a preliminary reference procedure), to provide answers to specific questions. In our submission, the EDPS emphasised the need to distinguish between Article 7 (*Respect for private and family life*) and Article 8 (*Protection of personal data*) of the EU Charter of Fundamental Rights. Both provisions are obviously closely related, but are different in nature. When determining the validity of legal acts under the Charter, the Court should therefore apply a double test, assessing whether the distinct requirements of both Articles 7 and 8 are fulfilled. Advocate General P. Cruz Villalón will deliver his opinion on 7 November 2013.

The EDPS pleadings

EVENTS

EDPS workshops on the use of mobile devices in the workplace and on websites

On 19 September 2013, we held two workshops on the use of mobile devices in the workplace and on websites managed by EU institutions and bodies. Over 60 participants attended each workshop, including data protection officers (DPOs), data protection coordinators (DPCs) and IT and communications experts. Prior to the meeting, we asked these colleagues from the EU institutions to take part in our survey to report on their own practices. This gave us a valuable insight into the experience and views on the issues that were subsequently debated, including the use of website cookies and private mobile devices in the workplace.

This was the second in a series of workshops that will help us to issue guidance on these and other technology-related subjects such as the use of electronic communications in the workplace and cloud computing, both of which are currently being prepared. The discussions in the workshops confirm the need for a common approach in protecting personal information and highlight the benefits of EU institutions and bodies exchanging experiences on good data protection practice, particularly in such complex and rapidly developing technological fields.

ERA Annual Conference on European Data Protection Law 2013

On 18 and 19 November 2013, the Academy of European Law (ERA) in Trier will hold its annual conference on European Data Protection Law. This year's conference will focus on the role of cloud computing services and social networks in applying EU data protection law. It will also be an occasion to update participants on the state-of-play of the reform process of EU Data Protection legislation and the most recent case law of the Court of Justice of the EU. The distinguished panel of speakers will be made up of lawyers, privacy advocates, academics, the European Commission and the EDPS, with Peter Hustinx giving a keynote speech. As key topics will include EU data sovereignty and cross-border data transfers to third countries as well as PRISM and data protection, the discussions are likely to be lively.

Conference programme

DATA PROTECTION OFFICERS

Recent appointments

- Ms. Christina Karakosta, ad interim, European Ombudsman (EO)

SPEECHES AND PUBLICATIONS

- Contribution (*pdf*) of Peter Hustinx at the LIBE Committee Inquiry on electronic mass surveillance of EU citizens, Public Hearing, Strasbourg (7 October 2013)
- Closing remarks (*pdf*) delivered by Peter Hustinx at the 35th International Conference of Data Protection and Privacy Commissioners, "Privacy: A Compass in Turbulent World", Warsaw (23-26 September 2013)
- Keynote speech (*pdf*) by Peter Hustinx at the Digital Enlightenment Forum, "Personal Data and Citizenship in the Digital Society", Brussels (19 September 2013)
- "(Future) Interaction between Data Protection Authorities and National Human Rights Institutions" article (*pdf*) by Peter Hustinx published in: "National Human Rights Institutions in Europe - Comparative, European and International Pesrpectives", Jan Wouters and Katrien Meuwissen (eds.), Cambridge 2013, p. 157-172 (17 July 2013)
- "Interesting Times for EU Data Protection", editorial (*pdf*) by Peter Hustinx in "L'Observateur de Bruxelles", nr. 93, p.5-6 (15 July 2013)

About this newsletter

This newsletter is issued by the European Data Protection Supervisor (EDPS) – an independent EU authority established in 2004 to:

- monitor the EU administration's processing of personal data;
- give advice on data protection legislation;
- cooperate with similar authorities to ensure consistent data protection

You can subscribe / unsubscribe to this newsletter via our website.

CONTACTS

www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
e-mail:
NewsletterEDPS@edps.europa.eu

POSTAL ADDRESS

EDPS
Rue Wiertz 60 – MTS Building
B-1047 Brussels
BELGIUM

OFFICE ADDRESS

Rue Montoyer 30
B-1000 Brussels
BELGIUM

Follow us on Twitter:
@EU_EDPS

EDPS - The European guardian of data protection