EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Newsletter

No. 40 | December 2013

IN THIS ISSUE

HIGHLIGHTS

Privacy and data protection can restore consumer confidence in the Digital Society

The European Commission's proposal on harmonising electronic communications services across the EU will unduly limit internet freedom, says the European Data Protection Supervisor (EDPS).

"Any monitoring and restriction of the internet activity of users should be done solely to achieve a targeted, specific and legitimate aim. The large-scale monitoring and restriction of users' internet communications in this proposal is contrary to EU data protection legislation as well as the EU Charter of Fundamental Rights. Such interference with the rights to personal data protection, confidentiality of communications and privacy will do little to restore consumer confidence in the electronic communications market in Europe."

Peter Hustinx, EDPS

EDPS Opinion

EDPS Press Release

TEN-T EA: ensuring the protection of whistle-blowers

European Commission | Trans-European Transport Network Executive Agency

Under the Staff Regulations of the EU institutions and bodies, staff who become aware of any facts that indicate illegal activity, including fraud or corruption, must inform their superiors. So that staff can report suspected illegal activities securely and in confidence, EU institutions and bodies have set up a procedure to protect whistle-blowers. In our Opinion of 28 October 2013, we analysed the draft procedure prepared by the Trans-European Transport Network Executive Agency (TEN-T EA) before its adoption and made the following recommendations:

- pointless and irrelevant information provided by whistle-blowers should not be retained longer than necessary;
- personal information processed should be limited to that data which is strictly necessary to verify the allegations;
- the confidentiality of whistle-blowers should be ensured by default, rather than on request; and
- the principle of confidentiality should be applied widely and broadly, not only in relation to the accused persons.

We welcomed how the procedure indicates what information is and is not relevant to the scope of the procedure, but stressed the importance of implementing stricter limitations and confidentiality of data in order to protect whistle-blowers. TEN-T EA finalised its procedure in line with our comments.

EDPS Opinion

SUPERVISION

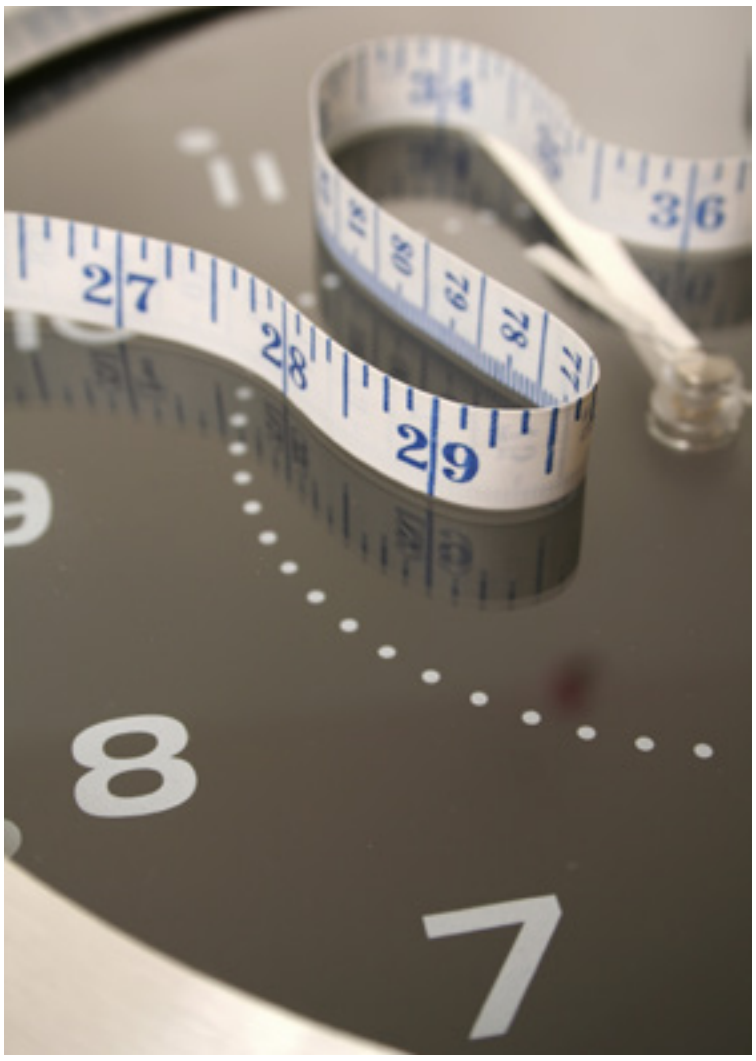
Guidelines on leave and flexitime: notifications on data processing operations

In December 2012, we published Guidelines on leave and flexitime. In these, the EDPS required EU institutions and bodies to submit notifications of processing operations which had not yet been analysed in order to ensure the correct implementation of data protection requirements within leave and flexitime processing operations. We have since received a total of 47 notifications on a range of processing operations. We responded to these with mini-opinions, which focus only on areas which differ from existing guidance.

Our analysis of these notifications has revealed that the main issue for all the operations is the length of time for which the collected data is retained. There was also an issue with the data protection clause that is to be signed by human resources staff. This clause is specifically linked to the processing of health data and we insisted that the staff concerned sign a declaration of confidentiality. We also highlighted the importance of giving staff and their family members all pertinent information about the operations, if they involve the processing of their personal information.

We have responded to all but a few of the notifications and have published or are in the process of publishing these on our website.

EDPS Guidelines



Ex-post prior checks - clearing the backlog

Ex-post prior checks refer to processing operations already in place, but also processing that began before 17 January 2004 (the appointment of the first EDPS and Assistant EDPS) or before the *Regulation* came into force. When the EDPS began his activities, there was a backlog of *ex-post* prior checking cases. As EU institutions and bodies have now had adequate time to notify their existing processing activities, we invited EU institutions and bodies to ensure all outstanding processing operations had been notified to us by the end of June 2013. Exceptions were made for certain activities carried out by recently-established bodies which would have been impossible to notify in advance, in cases of recruitment, for instance. As a result of this deadline, we received a total of 180 notifications between the beginning of June 2012 and the end of July 2013. 29 of these cases were found not to be subject to prior checking in 2013, in contrast to eight cases submitted inappropriately in 2012.

Creation of the Investigative Data Consultation Platform

The Investigative Data Consultation Platform (IDCP) is a project database which aims to facilitate exchange of information on anti-fraud investigations between OLAF and its international partner authorities. Once operational, the IDCP will allow users to verify whether specific information is included in partners' files, such as the names of persons under investigation, telephone numbers, addresses and so on.

In our Opinion we made several recommendations including:

- ensuring proper access rights for data subjects;
- reducing the period for which data is retained; and
- ensuring data quality.

Since IDCP activities entail structural transfers of personal data under Article 9 of *Regulation* 45/2001, the system cannot begin to operate without a separate authorisation by the EDPS under Article 9(7) of the Regulation. The IDCP will thus not become active until the EDPS grants such an authorisation.

EDPS Opinion

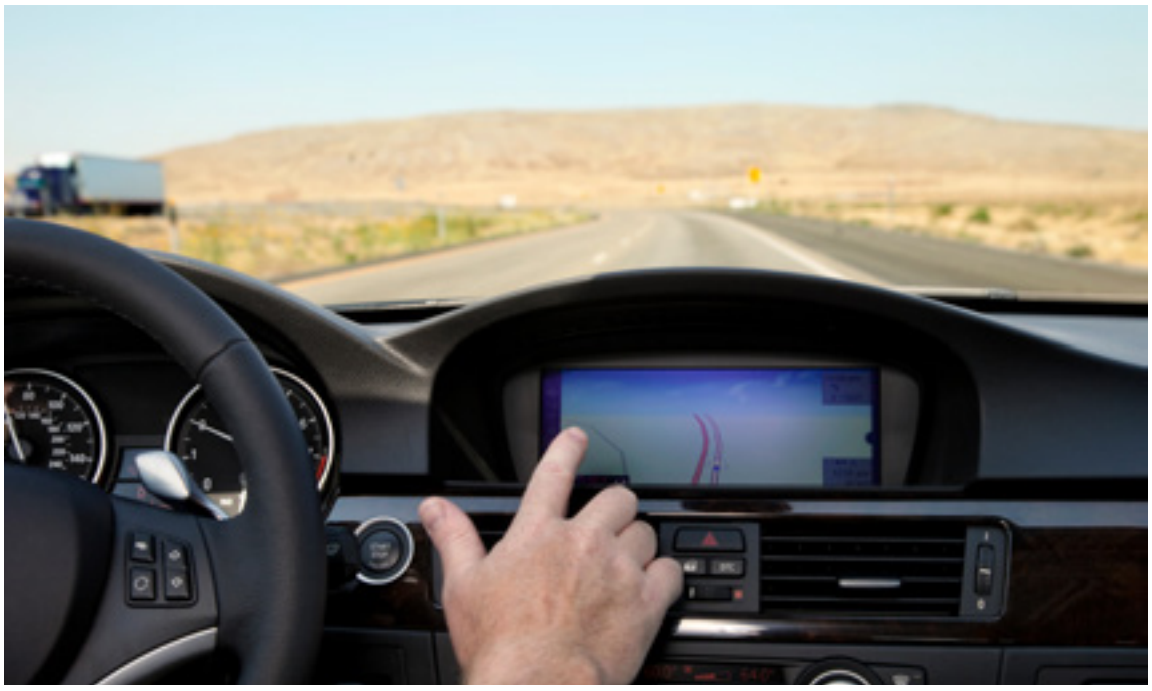
EUROPEAN ANTI-FRAUD OFFICE

CONSULTATION

Stressing safeguards for the eCall system

The 112 eCall system is an initiative intended to provide rapid assistance to motorists who are involved in a collision or accident within the European Union. In our Opinion of 29 October 2013 on the *Commission Proposal for a Regulation concerning type-approval requirements for the deployment of the eCall system*, we stressed the potential intrusiveness of the system. While we welcomed the specification within the Regulation for essential data protection safeguards, we insisted on the addition of complementary safeguards. By 1 October 2015, the fitting of eCall devices will be mandatory in all new vehicles. This broadening of deployment is expected to allow the eCall technology platform capabilities (positioning, processing and communication modules) to be *exploited commercially* (for example, advanced insurances schemes, stolen vehicles tracking, eTolling). Since this implies data protection risks, we emphasised the need for an equivalent level of data protection safeguards.

EDPS Opinion



EU-Canada PNR agreement: no take-off without data protection improvements

The Proposals for Council decisions on the agreement between *Canada and the EU on the transfer and processing of Passenger Name Records (PNR)* raise issues around necessity and proportionality. In our Opinion of 30 September 2013, we once again questioned the need for and scope of PNR schemes and bulk transfers of PNR data. We also questioned the legal basis for the agreement and expressed our concern at the apparent lack of independent redress available to EU citizens. We made several recommendations on issues such as:

- the exclusion of sensitive data processing;
- a reduced and justified retention period;
- a limited number of PNR data categories to be processed; and
- an explicit mention of the role of the independent authority as overseer.

EDPS Opinion

Keeping tabs on the data protection risks of eInvoicing

Across the European Union, public tender services are starting to require that invoicing should be done electronically. However, norms and standards on content, format, layout, technical requirements and other aspects of the invoicing vary considerably from one Member State to another. *The Commission Proposal for a Directive on electronic invoicing in public procurement* aims to encourage the use of e-invoicing and to improve interoperability between Member States. In our Opinion of 11 November 2013 on the proposal, we highlighted the increased privacy and data protections risks associated with making invoice data available in paperless and machine-readable form. We welcomed a move towards paperless eInvoicing, but warned that attention must be paid to issues such as the use of personal information beyond permissible limits, for automatic profiling or data-mining. Such uses are unlikely to be compatible with data protection rights or would require further safeguards.

EDPS Opinion

Taxation should not be at the expense of data protection and transparency

The Commission plans to amend its *Directive on the compulsory and automatic exchange of information in the field of taxation*, in order to expand its scope to include categories of information such as dividends, capital gains, other financial income and account balances. This extension will contribute to ensuring equality of treatment between different types of assets. In our letter to the Commission, we recommended that they should better define the type of personal information concerned and the purposes for which it can be exchanged. We also expressed our concern at the lack of provisions, either in the current Directive or the new proposal, for how the principle of transparency should be implemented in practice. We urged the legislator to consider issues of definition of types of personal information concerned, transparency, necessity and proportionality in this new proposal.

EDPS Comments

Risk assessment and security measures in EU institutions

Recent revelations about the surveillance and espionage activities of intelligences services in Member States and third countries suggest that the electronic communications of EU institutions and delegations have been targeted. There is also a concern that some security and cryptography tools on the market may have been intentionally weakened to make interception easier. In the light of these concerns, the EDPS wants to verify whether EU institutions still consider the risk assessment relating to their data protection operations to be valid and the current security measures appropriate. To that end, we are meeting with the European Parliament, Commission and Council to learn more about their reaction to the revelations and next steps.

Reflections on security: Internet designers fighting back against surveillance

The Internet Engineering Task Force (IETF), the body that designs the standards on which the internet works, came together in Vancouver on 3-8 November 2013 to brainstorm ways to improve the state-of-the-art in internet security. In early September, *The Guardian* published an *article* by Bruce Schneier, a well-known cryptographer, security expert and book author, who called upon internet engineers to take action and to dedicate that meeting to pervasive surveillance. It seems IT engineers have also had enough of the pervasive monitoring. After the revelations of this summer concerning the NSA and paying heed to Bruce Schneier's message, the IETF concluded that pervasive monitoring must be viewed as a technical attack and agreed to upgrade IETF standards. This is just one of many steps being taken in the wider internet community to develop solid technical countermeasures against this sort of surveillance. However, developing and publishing good technical specifications is only the first step. These need to be implemented and subsequently deployed to really enhance internet privacy. That may take some time and will need the participation of others.

Read more:

'Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security'

'Pervasive Monitoring is an Attack'

LinkedIn *Intro*: connect carefully

The professional social networking website, LinkedIn, has launched *Intro*, a new application for iOs Apple products. This application, which allows users to see LinkedIn profiles in their iPhone or iPad mail applications, redirects the user's emails through LinkedIn's servers. Here, LinkedIn profile metadata is added to the emails *Intro* users receive and the company essentially grants itself access to all email communications. The EDPS is concerned about the privacy risks of this application, as the email communications of *Intro* users are exposed and we strongly recommend that you do not install the app on your Apple device.

Read more about LinkedIn's *Intro* application on two security blogs by a third party security group by clicking *here* and *here*.

Uninstall Intro Guide, *LinkedIn FAQs* and *Privacy Statement*.

EVENTS

DPO Meeting

The 34th bi-annual Data Protection Officers' (DPO) meeting, hosted for the first time by the EDPS, took place in Brussels on 20-22 November 2013. The meeting focused on European and international data protection developments, emphasising the reform of the EU data protection legislation and the role of DPOs. The Director of the Commission's DG for Fundamental rights and Union citizenship, Mr Paul Nemitz, gave a presentation to the network of DPOs. A workshop was also organised on data protection and transparency, which gave rise to extensive and fruitful discussion. The EDPS updated the group on many areas of his work including prior checking procedures, Guidelines, first feedback from our 2013 Survey and the information of third parties in complaints. The meeting was also a useful forum for discussion on our future Guidelines on conflicts of interest, which the various DPOs participated in enthusiastically.

All the DPOs were willing to share their valuable views and front-line experience in matters of data protection. This undoubtedly contributed to the positive feedback and success of the meeting.

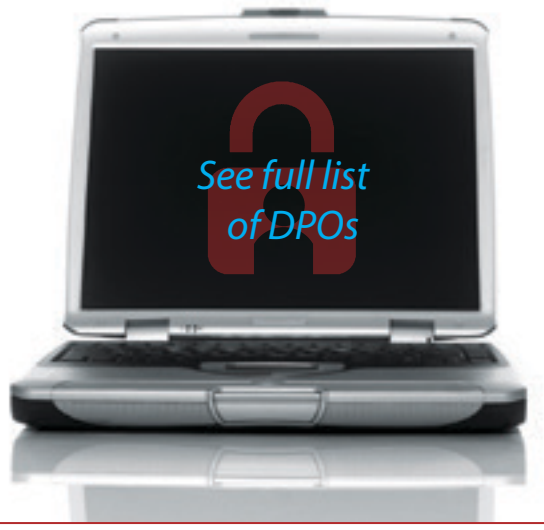
SPEECHES AND PUBLICATIONS

- Speech (*pdf*) delivered by Giovanni Buttarelli in Budapest, "Data Protection in the Judiciary: The Challenges for Modern Management" (24 October 2013)

DATA PROTECTION OFFICERS

Recent appointments

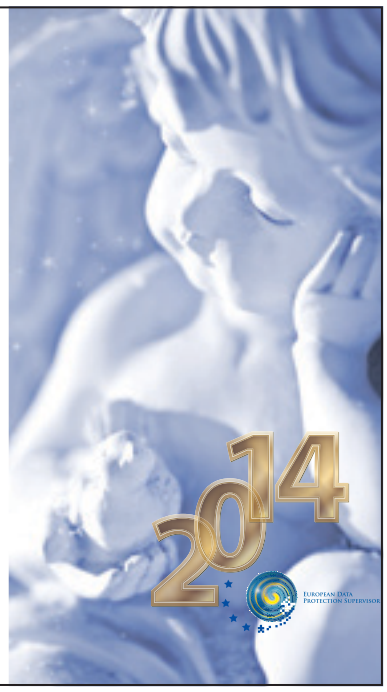
- Mr. Gabriele Borla, European Defence Agency (EDA)
- Mr. Nikolaos Chatzimichalakis, European Union Institute for Security Studies (EUISS)
- Mr. Andrej Gras, European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)
- Mr. Luca Zampaglione, ad interim, eu-LISA



Best wishes

Meilleurs voeux

Frohes Fest



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
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