

**CONSULTATION**

- > EDPS opinion on Agency for large-scale IT systems 2
- > EDPS reaction to adoption of ePrivacy Directive 2
- > EDPS opinion on combating fraud in the field of value added tax 3
- > Court intervention: right of access to EPSO pre-selection documents 4

**SUPERVISION**

- > News on EDPS prior checking of personal data processing 5

**EVENTS**

- > 4th European Data Protection Day - 28 January 2010 6
- > 3rd International Computers, Privacy and Data Protection Conference (29-30 January 2010) 7
- >> International Conference on Data Protection and Privacy Commissioners (Madrid, 4-6 November 2009) 7
- > "Responding to data breaches" Seminar (Brussels, 23 October 2009) 8

**SPEECHES AND PUBLICATIONS**

- 8

**NEW DATA PROTECTION OFFICERS**

- 9

Entry into force of Lisbon Treaty: impact on data protection



The Treaty of Lisbon which entered into force on 1 December 2009 has important consequences for data protection.

The Lisbon Treaty abolishes the pillar structure which, over the years, led to many questions relating to data protection and it creates a new legal basis for data protection, by introducing Article 16 in the Treaty on the Functioning of the European Union (TFUE). This new legal basis replaces Article 286 of the EC Treaty which was the basis for the establishment of the EDPS.

The new Article 16 upgrades the provision on data protection from a remote corner in the Treaty to Part I, Title II which contains general provisions of EU law (such as non-discrimination or public access to documents). It is general in scope since it applies at national and European levels to both the private and public sectors, including police and judicial cooperation. Under Article 16 of the TFEU everyone has a right to the protection of his or her personal data.

The Council and European Parliament shall lay down the rules on data protection. Until those new rules are adopted, the current framework for the former first pillar (mainly Directive 95/46/EC), the former third pillar (mainly Framework Decision 2008/977/JHA), and the processing by EU institutions (mainly Regulation (EC) Nr. 45/2001) will continue to apply.

Finally, an important development is the fact that the Charter of Fundamental Rights of the European Union, including its Article 8 on data protection, has become binding. Article 8 summarises the main elements of the fundamental right to data protection, such as purpose limitation, the right of access to and rectification of personal data, as well as independent supervision.



CONSULTATION

> EDPS opinion on Agency for large-scale IT systems



The EDPS opinion, adopted on 7 December 2009, relates to the Commission's proposed legislative package establishing an Agency for the operational management of large-scale information technology (IT) systems in the area of freedom, security and justice. The Agency would be responsible for the operational management of Schengen Information System (SIS II), Visa Information System (VIS), Eurodac and possible other large-scale IT systems.

As these databases contain large amounts of sensitive personal data (e.g. details of passports, visas and fingerprints), the EDPS analysed the proposal from a data protection standpoint, with a view of ensuring that certain possible risks, which could have great impact on the privacy of individuals, are sufficiently addressed in the founding legislative instrument.

The EDPS sees the advantages of setting up an Agency for the operational management of certain large-scale IT systems since it clarifies issues of liability and applicable law. He underlines, however, that such an Agency should only be established if the scope of its activities and its responsibilities are clearly defined. This is crucial to avoid the risk of function creep or the misuse of personal data.

“The creation of an Agency for such large-scale databases must be based on legislation which is unambiguous about the competences and the scope of activities of the Agency.” Peter Hustinx, EDPS

The EDPS encourages the legislator to take a cautious and restrictive approach. The point of departure should not be to bring as many large-scale IT systems as possible under the management of one Agency. Only after having acquired experience and following a positive evaluation of its functioning, other large-scale IT systems could be brought under the responsibility of the Agency. In order to improve the proposal, the EDPS recommends the legislator to:

- clarify whether the scope of activities of the Agency is limited to policies on border checks, asylum and immigration, or whether it should potentially cover all large-scale IT systems developed in the area of freedom, security and justice;
- clarify the notion of large-scale IT systems within this framework, and make clear whether it is limited to such systems which store data in a centralised database for which the Commission or the Agency is responsible.

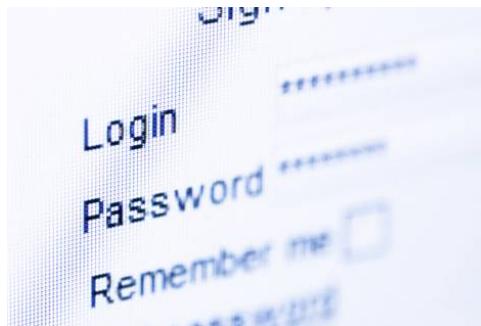
☞ EDPS opinion ([pdf](#))

> EDPS reaction to adoption of ePrivacy Directive

Following agreement on the EU telecoms reform at the beginning of November, nothing stands in the way for the ePrivacy Directive to enter into force. The revised Directive, as amended by the European Parliament and adopted by the Council, must be implemented by the Member States within 18 months.

The new provisions will bring vital improvements in the protection of the privacy and personal data of all Europeans active in the online environment. The improvements relate to **security breaches**, **spyware**, **cookies**, **spam**, and **enforcement of rules**. The EDPS cooperated closely with the

European Parliament, the Council and the European Commission on the legislative work leading to the final text.



The EDPS welcomes the many improvements in the protection of privacy in the revised ePrivacy Directive. He however points out that it is now crucially important to broaden the scope of the security breach provisions to all sectors and further define the procedures for notification. He notes in particular the emphasis on more effective enforcement of the rules on spyware and cookies. This has special relevance where privacy rights must be protected in relation to so called targeted advertising.

The changes introduced include:

- for the first time in the EU, a **framework for mandatory notification of personal data breaches**. Any communications provider or Internet service provider (ISP) involved in individuals' personal data being compromised must inform them if the breach is likely to adversely affect them. Examples of such circumstances would include those where the loss could result in identity theft, fraud, humiliation or damage to reputation;
- reinforced protection against interception of users' communications through the use of - for example - **spyware and cookies** stored on a user's computer or other device. Under the new Directive users should be offered better information and easier ways to control whether they want cookies stored in their terminal equipment;
- the possibility for any person negatively affected by **spam**, including ISPs, to bring effective legal proceedings against spammers;
- strengthened **enforcement powers** for national data protection authorities. They will for example be able to order breaches of the law to stop immediately and will have improved means of cross-border cooperation.

⇒ EDPS first ([pdf](#)) and second ([pdf](#)) opinions on the ePrivacy Directive review

> EDPS opinion on combating fraud in the field of value added tax



On 30 October 2009, the EDPS adopted an opinion on the Commission proposal to amend a Council Regulation on combating VAT fraud. With the amendment the Commission intends to enhance effectiveness of cross-border cooperation in this field and to improve collection and sharing of relevant information. The amendments also provide for a legal basis for setting up of a common operation structure for multilateral cooperation, called Eurofisc.

The EDPS concluded that not all requirements stemming from the Community rules on data protection were met. This is mainly due to the fact that provisions are formulated too broadly and leave too much room for discretion. A first issue is the use of the notion 'any information'. Such a broad notion opens the door for collection, storage and exchange of all kinds of personal information. The EDPS therefore asked the Council to specify and limit this notion.

The EDPS also pointed at the responsibility for compliance with data protection rules. The EDPS noticed that it is not always clear whether the Member States, the Commission or Eurofisc are responsible for such compliance. The EDPS called upon the Council to clarify this in the final text.

Uncertainty furthermore exists as regards the precise purposes for which competent authorities in the Member States exchange data about possible VAT fraud. The EDPS emphasised that these purposes should be clarified. He furthermore considered that the Council should make sure that data should only be used if it is necessary for the specified purpose. The EDPS also indicated that a maximum storage period should be determined.

One provision of the proposal addresses the issue of data protection. The EDPS was not satisfied with the proposed text as it does not meet the requirement that information is only used for the purpose for which it was collected. The provision furthermore allows for restrictions of data subject's rights in a way which is not consistent with the data protection rules.

☞ EDPS opinion ([pdf](#))

> Court intervention: right of access to EPSO pre-selection documents (Case Pachtitis v Commission)



On 1 December 2009, the EDPS intervened before the Civil Service Tribunal in the case Pachtitis v Commission. An agent of the EDPS pleaded in support of one of the applicant's pleas concerning EPSO's decision to reject his request to access some of the competition's documents, namely the questions that he answered. The EDPS argued that only if the applicant received the questions posed to him during the pre-selection tests, he would be able to evaluate his performance and verify EPSO's decision. That is why in essence he is entitled to have access to these data.

In his pleading the EDPS explained the purpose of the intervention, namely why the questions of the tests should be considered as personal data and why the applicant's request for access should be examined in the light of the Data Protection Regulation (Regulation (EC) No 45/2001) and not the Regulation on access to documents (Regulation (EC) No 1049/2001).

Furthermore, the EDPS counter-argued:

- the statement of the Commission that the Civil Service Tribunal is not competent to judge on issues relating to the Data Protection Regulation;
- the statement of the Commission that the Data Protection Regulation cannot be applied because Article 6 of Annex III of the Staff Regulations - according to which the proceedings of the Selection Board shall be secret - applies as *lex specialis*;
- the administrative requirement of the Commission to be able to use the questions in future competitions.

The EDPS concluded that since the Commission has not provided any legitimate reasons for justifying a restriction to the right of access (Article 20 of the Data Protection Regulation), it has infringed the fundamental right of access to the applicant's personal data.

☞ The whole text of the pleading can be found on the [EDPS website](#)



SUPERVISION

> News on EDPS prior checking of personal data processing

Processing of personal data by the EU administration that is likely to result in specific risks for the people concerned is subject to a prior check by the EDPS. This procedure serves to establish whether the processing is in compliance with the Data Protection Regulation (EC) No 45/2001, which lays down the data protection obligations of Community institutions and bodies.

>> Checking of flexitime clocking data



The envisaged processing within the framework of this prior check concerns the checking of Flexitime clocking against data on physical access to the Secretariat General of the Council (SGC).

The SGC uses a Flexitime system which manages working time and attendance. It facilitates the calculation of leave entitlement and checks the taking of leave as well as automatically calculates overtime. This application has already been prior checked by the EDPS.

The SGC also has a system of access control managed by the Security Office, which stores data in a database. This data is only accessible to the administration services within the framework of a formal administrative enquiry.

The comparison of the two sets of data aims to identify persons who transgress the Flexitime rules, and also to evaluate their behaviour. The system is also likely to lead to the adoption of disciplinary measures.

In his opinion released on 12 November 2009, the EDPS considered that the necessity and the proportionality of the checking of Flexitime clocking data against data on the physical access control system were questionable. According to the EDPS, there is no reasonable evidence showing that the implementation of a system of control comparing clocking times with data on physical access is necessary for the purposes of either personnel management or the functions of the SGC.

In his conclusions, the EDPS therefore considered that the envisaged processing would breach Regulation (EC) No 45/2001 at various levels (necessity and proportionality, change of purpose, quality of the data) if the checking of Flexitime clocking against data on physical access were carried out outside of the framework of an administrative enquiry.

☞ EDPS opinion (FR) ([pdf](#))

>> EAS Emotional Intelligence 360 degree assessment - Commission

The purpose of the processing activity in this case is to allow participants in the European Administrative School (EAS) training courses to obtain feedback, in the form of a report, to help them enhance their competences in the areas of self-management, relationship management and communication. The exercise is conducted with the use of a web-based tool: the "Emotional IntelligenceView 360". The report is generated automatically in response to the answers completed by the participants and his/her colleagues and does not reveal the way in which the colleagues completed the answers.

It has to be noted that even though the EAS has no access to the data processed by the contractor (data used by the company that run the tests for performing the Emotional Intelligence View 360), the contractor has to act according to the instructions given by the EAS. The EAS is the data controller of this processing activity. The contractor is therefore not authorised to make any further processing activity beyond what is determined by the EAS and specified in the contract.

In his opinion issued on 30 October 2009, the EDPS recommended the EAS, among other issues, to:

- explore the possibilities for making the use of this web-tool an anonymous exercise. In this regard, variables such as IT development, procedures and cost will have to be taken into account;
- include a clause in the contract with the processor specifying that the applicable law for the obligation of confidentiality and security of the processing carried out by the processor is the law of the Member State where the processor is established, in this case, the UK.

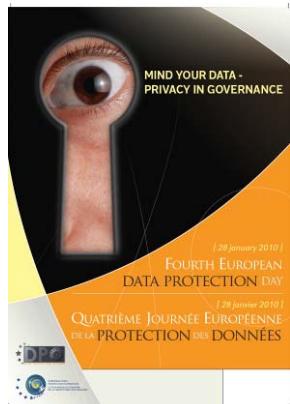
☞ EDPS opinion ([pdf](#))



EVENTS

> Forthcoming events

>> 4th European Data Protection Day, 28 January 2010



The Member States of the Council of Europe and the European institutions and bodies will celebrate the European Data Protection Day for the fourth time on 28 January 2010. This date marks the anniversary of the [Council of Europe's Convention 108 on the protection of personal data](#), the first legally binding international instrument related to the field of data protection.

The event will give the EDPS and Data Protection Officers the opportunity to focus on raising awareness among the EU staff about their rights and obligations regarding data protection - these rights and obligations are set out in Regulation (EC) No 45/2001 ([pdf](#)), the implementation of which is supervised by the EDPS.

To that end, a one-day **information stand** will be set up on three consecutive days in the Council (26 January), the European Commission (27 January) and the European Parliament (28 January).

To mark the event, Peter Hustinx, EDPS, will speak at a **lunchtime debate** entitled "Privacy and data protection: how does it affect you?" on 28 January. The presentation, which is mainly aimed at staff from the European Commission, will take place in DG Admin (Guimard) at 12h30.

The EDPS will also participate to the conference/award ceremony that will conclude the "**Think privacy**" campaign initiated by European Schoolnet and Microsoft in view of Data Protection Day. This second edition of the campaign features a Europe-wide "Think Privacy" contest where 15 - 19 year olds are invited to create and submit a multi-media presentation. This year's theme is "Privacy is a Human Right – treat it with care". Winners will be selected by a jury and invited to Brussels to attend the award ceremony on 28 January 2010 that will also be framed by keynotes of prominent policy makers.

☞ More information:

- [EDPS website](#)



- [Council of Europe website](#)
- ["Think privacy" campaign](#)

>> 3rd International Computers, Privacy and Data Protection Conference (Brussels, 29-30 January 2010)



Computers, Privacy and Data Protection – CPDP 2010 aims to create a bridge between policymakers, academics, practitioners and activists, exchange ideas and discuss emerging issues of information technology, privacy, data protection and law.

CPDP is organised by the *Vrije Universiteit Brussel*, the *Université de Namur*, the *Tilburg University*, the *Institut National de Recherche en Informatique et en Automatique* and the *Fraunhofer Institut für System und Innovationsforschung*.

Regular panel-sessions will be held with presentations by stakeholders (such as the European Commission and the data protection authorities), next to panel-sessions devoted to selected issues of information technology, privacy, data protection and law.

This year's conference theme will be "An Element of Choice" as a reference to the many options open for data protection policy.

Members of the EDPS secretariat will take part to panel discussions. Peter Hustinx, Supervisor, will provide the concluding notes to the conference.

☞ More information: www.cpdpconferences.org

> Outcome of past events

>> International Conference on Data Protection and Privacy Commissioners (Madrid, 4-6 November 2009)

In the line of the 2008 conference, the conference focused on new challenges raised by technological developments and the circulation of personal data in a global environment. The conference was an opportunity to observe a growing need, expressed by all actors including the civil society and industry, for a harmonised data protection framework across borders. It is in this spirit that the conference adopted a Resolution welcoming draft International Standards on the Protection of Personal Data and Privacy. These standards are the result of one year of preparatory work led by the Spanish authority. They represent the first step towards a binding international instrument.

The conference - at which Peter Hustinx, Supervisor, and Giovanni Buttarelli, Assistant Supervisor, both actively contributed - allowed for exchanges on new challenges in relation to security issues and the transatlantic dialogue between Europe and the United-States. Recent trends in the private sector were also discussed, such as behavioural advertising, the use of privacy by design, and the responsibility of controllers.

☞ More information at www.privacyconference2009.org

"Responding to data breaches" Seminar (Brussels, 23 October 2009)

The seminar, which was organised by the EDPS in cooperation with the European Network and Information Security Agency (ENISA), was mainly aimed at data controllers and data security practitioners. It was attended by more than 80 participants.

Introduced by keynote speeches from Supervisor Peter Hustinx, Commissioner Viviane Reding and ENISA Executive Director Udo Helmbrecht, discussions allowed to explore the challenges related to the main steps of the data breach life cycle: prevention, management and notification.

The debates highlighted the need for data controllers, together with other stakeholders, to adopt proper risk management in order to mitigate the risk of such breaches. It was stressed that this will not only require technological solutions but also organisational measures, including increasing the responsibility of the highest management levels of entities concerned. They should also promote the development of adequate safeguards and facilitate a more transparent distribution of responsibilities.

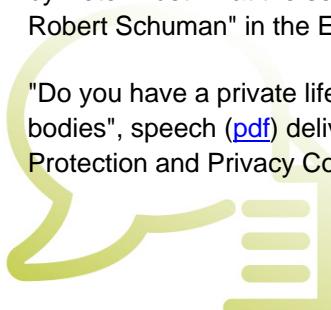
Although the obligation to notify breaches will be introduced in the revised "e-Privacy Directive", the seminar acknowledged that society's increasing reliance on information and communication technologies means that the data breach phenomenon already goes far beyond the electronic communications sector. In that sense, the Commission emphasised that, in close consultation with the EDPS and other stakeholders, it would consider going a step further than the e-Privacy Directive to extend the debate to generally applicable breach notification requirements and work on possible legislative solutions.

☞ More information on the [EDPS website](#)



S P E E C H E S A N D P U B L I C A T I O N S

- "Intelligent transport systems and data protection - ensuring the right balance between the protection of privacy and the efficient use of ICT in logistics", speech ([pdf](#)) delivered by Peter Hustinx at the CLECAT - 9th Freight Forwarders Conference (Brussels, 3 December 2009)
- "Ensuring trust in e-Health through strong health data protection", speech ([pdf](#)) delivered by Peter Hustinx at the European Policy Summit "Planning Europe's Healthcare Revolution" organised by Friends of Europe (Brussels, 2 December 2009)
- "Data protection integrated in an EU Information Management Strategy", speech ([pdf](#)) delivered by Peter Hustinx at the seminar on the Stockholm Programme organised by the "Fondation Robert Schuman" in the European Parliament (Brussels, 12 November 2009)
- "Do you have a private life at your workplace? Privacy in the workplace in EC institutions and bodies", speech ([pdf](#)) delivered by Giovanni Buttarelli at the 31st International Conference of Data Protection and Privacy Commissioners (Madrid, 6 November 2009)





NEW DATA PROTECTION OFFICERS

Each Community institution and body has to appoint at least one person as Data Protection Officer (DPO). These officers have the task of ensuring in an independent manner the application of the data protection obligations laid down in Regulation (EC) No 45/2001 in the concerned institution or body.

Recent appointments:

- **Frederik MALFRÈRE**, European Central Bank, in replacement of Martin BENISCH
- **Guido STÄRKLE**, European Railway Agency
- **Anne SALAÜN**, Artemis Joint Undertaking
- **Silvia POLIDORI**, Clean Sky Joint Technology Initiative
- **Estefania RIBEIRO**, Innovative Medicines Initiative Joint undertaking

☞ See full list of [DPOs](#).



About this newsletter

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

- monitor the EU administration's processing of personal data;
- give advice on data protection legislation;
- co-operate 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 34234234234
 Fax: +32 (0)2 34234234234
 e-mail: see our contacts page

POSTAL ADDRESS

EDPS – CEDP
 Rue Wiertz 60 – MO 63
 B-1047 Brussels
 BELGIUM

OFFICE

Rue Montoyer 63
 Brussels
 BELGIUM

EDPS – The European guardian of personal data protection