



EDPS NEWSLETTER

Issue n° 12 - 20 December 2007

The EDPS electronic newsletter can be [subscribed to](#) on our website at:
www.edps.europa.eu

Content:

1. [EDPS Opinion on EU-PNR](#)
2. [EDPS Opinion on RFID](#)
3. [Implementing rules of Prüm Initiative - EDPS Opinion](#)
4. [Judgment of CFI in Bavarian Lager vs. Commission](#)
5. [EDPS wishes to intervene in case on access to EPSO documents](#)
6. [Priority List Inventory](#)
7. [EDPS report on EURODAC security audit](#)
8. [EDPS issues comments on employee Internet monitoring policy](#)
9. [News on EDPS prior checking of personal data processing](#)
10. [Data Protection Day: 28 January 2008](#)
11. [New Data Protection Officers](#)
12. [Colophon](#)

1. EDPS Opinion on EU-PNR

On 20 December 2007, the EDPS issued an Opinion on the Commission's proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes. The proposal involves obligations for air carriers to transmit data about all passengers on flights to or from an EU Member State.

The Opinion emphasizes the major impact the proposal would have on privacy and data protection rights of air passengers. While acknowledging that the fight against terrorism is a legitimate purpose, the EDPS expresses serious concerns about the necessity and proportionality of the proposal which, in his view, are not sufficiently established in the proposal. In addition, the EDPS takes a critical stance on the lack of clarity in relation to various aspects of the proposal, in particular the applicable legal framework, the identity of the recipients of personal data, and the conditions of transfer of data to third countries.

The Opinion focuses on four key issues and draws the following conclusions:

- **legitimacy of the processing:** the proposal does not provide for sufficient elements of justification to support and demonstrate the legitimacy of the processing of data;
- **applicable legal framework:** a significant lack of legal certainty is noted as regards the regime applicable to the different actors involved in the matter;
- **the identity of data recipients:** the draft Decision does not provide for any specification concerning the identity of the recipients of personal data collected by airlines companies;
- **transfer of data to third countries:** it is imperative that conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection.

Finally, the EDPS advises not to adopt the draft Decision before the new Lisbon Treaty's entry into force, so that it can follow the co-decision procedure foreseen by the new Treaty and the European Parliament is fully involved.

🔗 [EDPS Opinion on EU-PNR \(pdf\)](#)

2. EDPS Opinion on RFID

The EDPS published on 20 December 2007 an Opinion on the Commission's Communication on Radio Frequency Identification (RFID) in Europe that was released in March 2007. The Opinion deals with the growing use of RFID chips in consumer products and other new applications affecting individuals.

The EDPS welcomes the Commission's Communication on RFID as it addresses the main issues arising from the deployment of RFID technology while taking account of privacy and data protection considerations. The EDPS

agrees with the Commission that it is appropriate in the first phase to leave room for self-regulatory instruments. However, additional legislative measures may be necessary to regulate RFID usage in relation to privacy and data protection.

Supporting the opt-in option at the point of sale, the "privacy by design" principle and the identification of "best available techniques", the EDPS recommends considering the adoption of a proposal for Community legislation regulating the main issues of RFID-usage in case the proper implementation of the existing legal framework fails.

☞ EDPS Opinion on RFID ([pdf](#))

3. Implementing rules of Prüm Initiative - EDPS Opinion

On 19 December, the EDPS presented his opinion on the German initiative establishing implementing rules which are necessary for the functioning of the Council Prüm initiative. The EDPS already issued an opinion ([pdf](#)) on 4 April on the Council Prüm initiative, which aims to step up cross-border cooperation, particularly for combating terrorism and cross-border crime, by establishing mechanisms to exchange personal data such as DNA profiles and fingerprints.

The implementing rules and their annex vest a specific importance since they define crucial aspects and tools of the exchanges of data that are essential to ensure guarantees for concerned persons. Furthermore, the current lack of a general EU framework that would guarantee harmonized data protection in the law enforcement sector calls for specific attention in these rules.

In particular, in this opinion the EDPS recommends that:

- the combination of general provisions and specific tailored rules on data protection should ensure both the rights of citizens and the efficiency of law enforcement authorities when the proposal enters into force;
- the accuracy in searches and comparisons of DNA profiles and fingerprints should be duly taken into account and constantly monitored, also in the light of the larger scale of the exchange;
- relevant data protection authorities should be put in a position to properly carry out their supervisory and advisory role throughout all the different stages of the implementation.

☞ EDPS Opinion on implementing rules of Prüm initiative ([pdf](#))

4. Judgment of the Court of First Instance in Bavarian Lager vs. Commission (T-194/04)

On 8 November 2007, the Court of First Instance (CFI) issued a judgment on a case relating to the balance between two fundamental rights: the right of access to documents of the EU institutions and the right to data protection. The judgment is an important milestone in the debates on this balance.

The CFI annulled the Commission's decision to refuse full access to the minutes of a meeting organised by the Commission, including the names of the participants of that meeting. The CFI held that disclosure of names of representatives of a collective body would not jeopardise the protection of their privacy and integrity.

The EDPS had intervened in the case in support of the applicant for access and had defended a position that was in substance confirmed by the CFI.

The Commission will now decide whether to issue an appeal at the Court of Justice.

☞ [Case T-194/04: Bavarian Lager vs. Commission](#)

5. EDPS wishes to intervene in case on access to EPSO documents (T-374/07)

The EDPS has requested to be allowed to intervene in a case on access to certain documents of an [EPSO](#) (European Personnel Selection Office) competition at the Court of First Instance.

The applicant in this case had participated in a competition for administrator linguists with Greek as main language and requested a copy of the tests he had taken as well as of the correct answers. This request was refused by EPSO.

The issue of access by candidates in a competition to the results of their tests and related documents has been the subject of several prior checks by the EDPS.

☞ [Case T-374/07: Pachtitis vs. Commission and EPSO](#)

6. EDPS Inventory 2008 (legislative consultation) has been published

The second public inventory of the EDPS as an advisor on proposals for legislation and related documents was published on the EDPS website.

This inventory forms part of the annual work cycle of the EDPS. Once a year the EDPS reports retrospectively on his activities in the Annual Report. In

addition, the EDPS publishes an inventory of the intentions of the EDPS in the area of consultation for the next year.

The main source of the inventory is the Commission's Work Programme for 2008 ([pdf](#)). The inventory consists of an introductory part which includes the priorities for the EDPS for 2008, as well as an annex of the relevant Commission-proposals and other documents that require the attention of the EDPS.

As one of the priorities for 2008, the EDPS will look at the consequences of the entry into force of the Lisbon Treaty for data protection.

➤ [EDPS Inventory 2008](#)

7. EDPS report on EURODAC security audit

As the supervisory authority of the Central Unit of EURODAC, the EDPS launched a comprehensive inspection of the EURODAC system which was completed in March 2006. This was followed by a decision to initiate an in-depth security audit, the results of which were presented to the European Commission on 9 November 2007.

The security measures initially implemented with respect to the EURODAC system and their management have provided a fair level of protection to date. However, some parts of the systems and the organizational security present some weaknesses which will have to be addressed in order for EURODAC to fully comply with best practices and the implementation of best available techniques.

The EDPS will review the proper implementation of the follow-up measures which will be elaborated on the basis of the present report.

Although the report is EU Restricted, a short summary ([pdf](#)) is available on the EDPS website.

8. EDPS issues comments on employee Internet monitoring policy

In response to a consultation request from the European Court of Auditors, on 26 November 2007 the EDPS submitted comments on the Court's Draft Internet Security Policy. Under Article 28(1) of Regulation (EC) 45/2001 ([pdf](#)) the EDPS has the right to be informed of administrative measures related to the processing of personal data and to provide guidance on these measures.

The EDPS' remarks focussed on various issues. He emphasized the importance of transparency and stressed the need for the Court to use all available means, on-line and off-line, to communicate to and raise awareness

among employees of the Internet Security Policy. On the use of consent to legitimise Internet monitoring, the EDPS expressed doubts as to whether the Court employees were in a position to make a real, freely given choice as to the monitoring of their Internet usage.

On the use of the Internet for private purposes, the EDPS considers a policy of zero tolerance to be impractical and unrealistic. The EDPS favoured the setting up of clear limits, such as the allocation of time slots for the use of Internet for private purposes, between 12 and 2 pm and before 8 am or after 6 pm for example.

In addition, the EDPS favoured the use of filter software which entails a preventive approach to the misuse of the Internet rather than a detective one. On the conditions for the monitoring of Internet usage, he endorsed the setting up of clear limitations guaranteeing that monitoring only takes place when it is absolutely necessary and for specified purposes. He approved measures such as sporadic rather than permanent monitoring and the monitoring of traffic volume by department rather than by individual usage. He recommended the setting up of limitations on the storage of log files (maximum of six months).

☞ EDPS comments on the Court of Auditors' Internet security policy ([pdf](#))

9. 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 (the data subjects) is subject to a prior check by the EDPS. This procedure serves to establish whether or not the processing is in compliance with Regulation 45/2001, which lays down the data protection obligations of the EU institutions and bodies.

9.1 OLAF "Information and Intelligence Data Pool" and Intelligence Databases

"Information and Intelligence Data Pool" is the description given to all data held within the remit of Operational Intelligence Unit C4 in OLAF, including the Intelligence Databases.

Operational Information and Intelligence support are essential aspects of OLAF's mandate to fight fraud, corruption, and any other illegal activity affecting the financial interests of the European Community, and serious matters relating to the discharge of professional duties - as established in Article 1 of Regulation (EC) n° 1073/1999 ([pdf](#)) and Commission Decision 1999/352/EC Article 2 (5) ([pdf](#)).

The purpose of the processing under analysis is to further OLAF's intelligence/analysis and operational activity. It also aims to support specific case requests, operations and investigations with a view to ensuring the optimum accuracy and relevance of information received, disseminated and

otherwise processed for intelligence, financial, administrative, disciplinary and judicial use. This support may be provided throughout the various stages of OLAF investigation and operational activities, over all sectors and is recorded within the CMS (Case Management System) where applicable.

In his prior checking Opinion of 21 November 2007, the EDPS issued the following main recommendations:

- to acknowledge in the intelligence files when any restriction based on Article 20 of the Regulation is applied;
- to respect the confidentiality of the identity of whistleblowers during OLAF intelligence activities and in the later stages when appropriate;
- to provide the information (Article 12 of the Regulation) to the data subjects whose names appear in the documentation under analysis, but who are not persons concerned, witnesses, whistleblowers or informants, unless such activity would be impossible or would involve a disproportionate effort, in which case the obligation to provide directly the information could only be replaced by the indirect provision through the privacy statement published on the OLAF website. The same principle should be applied when intelligence activities are conducted independently of an investigation;
- to supplement the publication on the website with personalised information notices addressed to individuals (unless such activity would be impossible or would involve a disproportionate effort). The EDPS therefore called upon OLAF to develop practices in providing personalised information to the individuals concerned to the degree to which it is appropriate in the context of intelligence activities and inform the EDPS about such guidelines.

↪ EDPS Opinion on OLAF Intelligence databases ([pdf](#))

9.2 Flexitime - specific to DG INFSO

On 19 October 2007, the EDPS adopted an Opinion on "the implementation of flexitime - specific to DG INFSO".

Within the general framework of Time management regulated by the "[SYSPER 2 Time management system](#)", DG INFSO added to the application of the flexitime system an important component in the form of an RFID chip integrated in the personal badge necessary to clock in and out. The inclusion of such a technology into a flexitime system thus reinforces the specific risks already present in the system. Therefore, the EDPS considered the case as such subject to prior checking.

In his analysis, the EDPS concluded that the system does process personal data because the data on the use of badges relate to natural persons who are identifiable, for instance by the use of names and identification numbers. Furthermore, the EDPS closely analysed the necessity test applied to the

system and concluded that there was no specific need to develop a badging system using RFID to implement a flexitime system, as the same purpose (management of working hours) could be reached by other, less intrusive, means.

However, the EDPS also accepted that a margin of appreciation was left at the discretion of the administration in deciding to implement this system using RFID. Provided that adequate safeguards and proportionality are present, it can be considered that such a system fulfils the conditions of need.

In his conclusions, the EDPS requested several modifications to the planned system regarding security aspects and in the meantime, approved a temporary solution. The other recommendations concerned the drafting of the privacy statement, some organisational measures and the categories of data subjects concerned.

☞ EDPS Opinion on the implementation of flexitime - specific to DG INFSO ([pdf](#))

10. Data Protection Day: 28 January 2008

The Member states of the Council of Europe and the European institutions will celebrate the Data Protection Day for the second time on 28 January 2008. This date marks the anniversary of the [Council of Europe's Convention 108](#); the first legally binding international instrument related to the data protection field.

The [Council of Europe's website](#) provides for a page dedicated to the event from which you can access - via the country flags list - all the various initiatives that have been or will be undertaken across Europe to commemorate Europe's second Data Protection Day.

The event will give the EDPS the opportunity to focus on raising awareness among MEPs and EU staff about their rights and obligations regarding data protection. A one-day information stand will be set up in the European Parliament, the European Commission, and the Council premises.

The EDPS will outline his supervisory, consultative and cooperative roles, as well as his achievements and current activities. A number of communication tools and multimedia material will be used as a support. A quiz will also be made available on the spot as well as on the EDPS website for download.

☞ **Practical information:**

- European Parliament: 28 January 2008 ; 11.00 - 15.00
ASP Building, main street
- Council: 29 January ; 11.00 - 15.00

Justus Lipsius Building

- European Commission: 30 January ; 11.00 - 15.00
Berlaymont Building, main entrance hall

11. New Data Protection Officers

Each EC 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 internal application of Regulation 45/2001.

Recent appointments:

- Terry TAYLOR, European Agency for Safety and Health at Work (EU-OSHA);
- Jobst NEUSS, European Investment Fund (EIF);
- Arthur BECKAND, European Aviation Safety Agency (EASA);
- Martin DISCHENDORFER, European Agency for Reconstruction (EAR).

☞ See full list of [DPOs](#).

12. Colophon

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.

Postal address:

EDPS - CEPD
Rue Wiertz 60 - MO 63
B-1047 Brussels
BELGIUM

Office:

Rue Montoyer 63
Brussels
BELGIUM

Contact details:

Tel: +32 (0)2 283 19 00

Fax: +32 (0)2 283 19 50

e-mail: see [contact page](#) on the website

EDPS - the European guardian of personal data protection

www.edps.europa.eu