# EDPS Newsletter

No 38 | JUNE 2013

EUROPEAN DATA PROTECTION SUPERVISOR



## - HIGHLIGHTS -

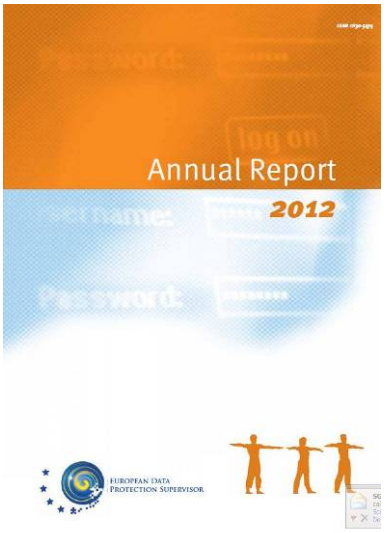
## > Strong data protection to improve EU approach to serious crimes

Robust data protection considerations can strengthen the **credibility** of investigations into **serious crimes** in the EU. This is the message the European Data Protection Supervisor (EDPS) sent in his opinion published on 3 June 2013, on the Commission proposal for a new legal framework for the EU Agency for Law Enforcement and Training (Europol). The EDPS fully supports the need for innovative and flexible approaches in preventing and combating serious crimes, but also insists on **strong safeguards**. The validity of a criminal investigation relies on the quality and integrity of the data collected. Respecting data protection principles can help reinforce the **reliability** of such evidence.

> ***A strong framework of data protection is important not only for those under suspicion or involved in an investigation, but also contributes to the success of police and judicial cooperation. As the work of Europol relies on the cooperation with and between law enforcement agencies in Europe, it is important that data protection considerations are fully taken into account: in practice this means that Europol should collate personal information for specific investigations only. It is important that Europol maintains a high level of data protection as the role it plays in combating serious crimes increases. The effective supervision of Europol is needed to ensure that it operates in full compliance with the stringent case law of the EU Court.***

☞ EDPS Opinion (pdf) and press release (pdf)

## > 'Smart, sustainable, inclusive Europe': only with stronger and more effective data protection




On 29 May 2013, the EDPS presented his **Annual Report** of activities for 2012 to the Committee on Civil Liberties, Justice and Home Affairs (LIBE) at the European Parliament.

At the animated press conference that followed, Peter Hustinx, EDPS, spoke of the exceptional lobbying surrounding the current **review** of the **EU data protection law** by organisations both from Europe and elsewhere. He warned the EU legislator to **guard against** undue pressure from industry and third countries to lower the level of data protection that currently exists and instead seize the opportunity to ensure **stronger** and **more effective protection** to individuals across the EU.

The current legislation for data protection was adopted 18 years ago at a time when the internet barely existed. An update is long overdue and the EDPS is closely involved in the ongoing work on the reform. The review process has attracted enormous attention from industry alleging that data protection rules are a hindrance to innovation.

> ***"The benefits for industry should not - and do not need to - be at the expense of our fundamental rights to privacy and data protection. The integration of data protection principles in technical innovation or in the transfer of our personal information to relevant bodies, in the interests of security for example, can add significant value, both in terms of efficiency and lower costs, if privacy is built into the design of processes from the outset."***
>
> ***Peter Hustinx, EDPS***

☞ EDPS Annual Report 2012 (pdf), executive summary (pdf) and press release (pdf)

# CONSULTATION

## > Credible cyber security strategy in the EU needs to be built on privacy and trust

Cyber security is not an excuse for the **unlimited** monitoring and analysis of the personal information of individuals, said the EDPS on 17 June 2013, following the publication of his **opinion** on the **EU's strategy on cyber security**. While there is a welcome acknowledgement of the importance of data protection principles for a robust cyber security policy, the strategy is **not clear** on how these principles will be applied in practice to

reinforce the security of individuals, industry, governments and other organisations.

Peter Hustinx, EDPS, said: "There is no security without privacy. So I am delighted that the EU strategy recognises that it is not a case of privacy versus cyber security but rather privacy and data protection are guiding principles for it. However, the ambitions of the strategy are not reflected in how it will be implemented. We acknowledge that cyber security issues have to be addressed at an international level through international standards and cooperation. Nevertheless, if the EU wants to cooperate with other countries, including the USA, on cyber security, it must necessarily be on the basis of mutual trust and respect for fundamental rights, a foundation which currently appears compromised."

☞ EDPS Opinion (pdf) and press release (pdf)

## > A closer look at Market Surveillance

The aim of the Commission's proposed Regulation on the market surveillance of products (which also amends various legislative instruments) is to ensure that products do not endanger health, safety or any other aspect of public interest and that they comply with the requirements set out in the EU product harmonisation legislation.

The proposal is a good example of a legislative proposal with significant data protection implications that may not be immediately obvious. In our opinion of 30 May 2013, we stressed that a proposal should always consider whether EU data protection rules are applicable, especially where the sharing of information is allowed for, whether through dedicated IT platforms or not. As a rule, whenever a legislative proposal involves the processing of personal information, even if it is not the main purpose, national rules implementing the data protection Directive 95/46/EC and/or regulation (EC) No 45/2001 are applicable. Certain conditions apply, therefore, whenever personal information is to be collected, analysed or processed. For example, only personal information that is strictly necessary for the stated purpose should be collected and specific time-limits for the retention of the information collected should be set. We also highlighted that where the personal information of an economic operator (e.g. the manufacturer, their authorised representative, the importer and/or the distributor of a product available on the EU market) is to be made public, the kind of personal data that is to be published and the reasons for doing so must be made explicit in an advance privacy notice to those concerned.

☞ EDPS Opinion (pdf)

## > Regulating the prices of medicinal products for human use

On 30 May 2013, we adopted an Opinion on the amended Commission proposal for a Directive on the *transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of public health insurance systems.* The aim of the proposal is to ensure that national rules on pricing and reimbursement of medicines do not oppose the principle of free movement of goods in the EU. We emphasised that personal information processed in the context of the pricing and reimbursement procedures of national health authorities may relate to patient health data. As a

consequence, a higher level of data protection is required. We recommended that any patient health data included in data that is submitted by a pharmaceutical company in order to be authorised to put a medicinal product on the market is fully anonymised - in other words, that the identity of the person cannot be determined - before this data is transferred to the national health authorities for any further processing. We also questioned the necessity and proportionality of the mandatory publication of names and declarations of interest of experts, members of decision making bodies and members of bodies responsible for remedy procedures.

☞ EDPS Opinion (pdf)

## > Strengthening law enforcement cooperation in the EU: the European Information Exchange Model

On 29 April 2013, we adopted an Opinion on the Commission Communication *Strengthening law enforcement cooperation in the EU: the European Information Exchange Model* (EIXM). We were pleased that the Communication concludes that neither EU-level law enforcement databases nor new EU information exchange instruments are needed. However, we emphasised the need for a full evaluation process of the existing instruments and initiatives in the Justice and Home Affairs area, the outcome of which should lead to a comprehensive, integrated and well-structured EU policy on information and exchange management.

☞ EDPS Opinion (pdf)

## > Data protection integral to cooperation on narcotics

On 23 April 2013, we adopted an opinion on the Commission proposal for the conclusion of an agreement between the EU and the Russian Federation on drug precursors. The aim of the agreement is to increase cooperation to prevent legal substances from being used to illicitly manufacture narcotic drugs and psychotropic substances (called drug precursors). The agreement will, for instance, allow the transfer of personal information on suspect transactions of drug precursors.

We welcomed the provisions on personal data protection in the text of the agreement and the inclusion of mandatory data protection principles in the annex. However, we are concerned about the actual enforceability of these principles, so we recommended that EU and Russian data protection authorities jointly review the implementation of the agreement. We also recommended that the text explicitly allows for the possible suspension or termination of the agreement if data protection principles are breached.

In addition, we advised better specification of data protection safeguards, for example the purpose of the transfers of personal information, the retention periods, the categories of data to be exchanged and the protection of data relating to suspect transactions. In the interests of completeness of the

mandatory data protection principles, we recommended adding provisions relating to sensitive data, data security and the restriction of the onward transfers of personal information.

☞ EDPS Opinion (pdf)

# SUPERVISION

## > EIGE: towards data protection

On 22 May 2013, Giovanni Buttarelli, Assistant EDPS, visited the European Institute for Gender Equality (EIGE) in Vilnius, Lithuania with a view to improving compliance with data protection rules at the agency.

EIGE became operational in the summer of 2010 and has not yet achieved the benchmark standard set by its peers. To date, the agency has failed to submit any Article 27 notifications. Under Article 27 of the Regulation, any processing of personal information at an EU institution or body that presents specific risks to the rights and freedoms of individuals is subject to prior-checking by the EDPS.

The visit included meetings with management, staff and the data protection officer to raise awareness and provide guidance. In conclusion, the management of EIGE agreed to a roadmap of precise data protection activities and targets with the EDPS that should help to remedy its current shortcomings.

## > Clarifying the scope of the compatible use of personal information at EIB

The European Investment Bank (EIB) consulted us on the legality of analysing information from an access security system or from a time management system for another purpose, namely for investigations to instruct disciplinary procedures.

In our analysis of 17 April 2013, we stressed that the concept of purpose limitation is an essential first step in applying data protection law. Purpose limitation means that personal information may only be collected for specified, explicit and legitimate purposes. It contributes to transparency, legal certainty and predictability and aims to protect individuals by setting limits on how their information is used. Nevertheless, it also offers a degree of flexibility to the EIB.

Following an analysis of the rules governing disciplinary procedures and fraud investigations at the EIB, we concluded that these rules could allow the use of such information in disciplinary investigations and be compatible with these purposes. However, such authorisation is limited to these purposes and the proportionality and necessity of the processing of the information must be

respected. Furthermore, the re-use of this information for another purpose should only be permitted in the context of an open disciplinary process for a specific case and is not an opportunity for a fishing operation - an attempt to discover the facts about something by collecting a lot of information, often on unrelated or minor matters or in secret.

This is the second of two recent cases that we have analysed that relate to the definition of compatible use and demonstrates a possible trend in the further use of information that was originally collected for a another purpose. See also our non-prior check case on EFSA of 9 April 2013.

☞ EDPS Opinion (pdf)

## > Transfers of staff data to Permanent Representations

The data protection officer (DPO) of an EU Agency consulted the EDPS on the transfer of personal staff data to the Permanent Representation of Member States. (The main responsibility of Permanent Representatives is to collectively prepare the work of the Council of the European Union as part of the COREPER committee).

In his reply of 9 April 2013, the EDPS pointed out that such requests should always specify a purpose and be subject to a clear legal basis, for instance Article 15, second subparagraph of Protocol No. 7 to the Treaty on the Functioning of the European Union (TFEU) on the privileges and immunities of the EU, providing that the names, grades and addresses of officials and other staff in certain categories "shall be communicated periodically to the governments of the Member States".

It appears that this is a widespread issue and so on 8 May 2013, the EDPS launched a survey to gather more information from DPOs about such transfers in other EU institutions, bodies and agencies.

☞ EDPS Opinion (pdf)

## > Declarations of interests: a balance between privacy and transparency

On 8 March 2013, the European Joint Undertaking for ITER and the Development of Fusion Energy (F4E) notified us of its processing operations on the declarations of interests of the members of its Executive Committee. Such declarations safeguard the independence of these members and avoid any conflicts of interest which could interfere with their activities. The declarations contain information on current and former employment, investments or grants received by members as well as spouses, partners or household members. These declarations of interests can be made public upon request.

In our opinion of 30 May 2013, we said that such publication can be justified to allow control by peers and the public depending on the tasks of the members of the Executive Committee.

However, as in other similar cases (such as ECDC reported on in our December 2012 newsletter), we recommended that the agency take a proactive

approach in such issues of transparency. Institutions and bodies should assess the potentially public nature of personal information when collecting it and properly inform the individuals concerned about its possible disclosure and their right to object (in a privacy notice, for example).

We also pointed out that the disclosure of declarations of interest is in effect a transfer of data. As set out in the EDPS paper on *Public access to documents containing personal data after the Bavarian Lager ruling,* an institution needs to take into account the legitimate interests and views of the individual(s) concerned in order to balance the interests of all concerned and make a well-informed decision. In our view, consent is not necessary as the balance of interests in this instance would be devoid of substance otherwise. Nevertheless, individuals have the right to object to the publication on compelling and legitimate grounds.

☞ EDPS Opinion (pdf)

## > Clarifying the scope of the compatible use of personal information at EFSA

In our reply of 9 April 2013 to a prior-check notification from the European Food Safety Authority (EFSA) on the use of access badge information for staff presence in the office, we concluded that this operation was not subject to prior-checking.

However, as per the consultation of EIB described above, this case allowed us to clarify the compatible use of information originating from an access control system.

We highlighted the importance of the purpose limitation principle, which means that in each situation where the further use of personal information is considered, a distinction must be made between additional uses that are 'compatible' and other uses, which should remain 'incompatible'. For instance, the potential to link an access control database with a time management database would not be compatible.

In this case, the use could be considered compatible in view of helping jobholders. However, we expressed doubts as to the necessity of implementing such system, as other means are available that do not require the use of records from the access control system.

☞ EDPS Opinion (pdf)

# EVENTS

## > EDPS workshop on electronic communications, Brussels

On 12 June 2013, we organised a workshop on the use of electronic communication in the workplace. 75 participants including data protection officers (DPOs), data protection coordinators (DPCs) and staff from the IT and HR fields represented the majority of EU institutions and bodies. They offered valuable contributions on the experience gathered from their day-to-day work in the use of phones, internet and email. Other meetings and email contact with DPO/DPC networks, IT, HR and staff from other fields within the EU administration will help to gather other pertinent information.

This was the first in a series of initiatives that will help us to prepare guidance on this subject and other examples of electronic communication (including mobile device usage, cloud computing and EU websites) which we hope to finalise by the end of the year, and we plan to organise similar workshops later in the year.

The high level of attendance at this workshop confirms the importance of the subject and the key role of inter-institutional cooperation in addressing such issues.

## > Meeting of the Customs Information System supervision coordination group, Brussels


The sixth meeting of the Customs Information System (CIS) supervision coordination group took place on 11 June 2013. As the mandates of the Chair and Vice Chairman expired on 7 June 2013, an election was held by means of a secret ballot at this meeting. Mr. Giovanni Buttarelli, Chair of the Group, and Mr. Gregor Konig, Vice-Chair of the group, were both re-elected.

The group also studied the draft report on the coordinated inspection of the list of authorities having access to CIS and FIDE and the draft report on CIS data subject's rights. The next meeting of the group is likely to be in the Autumn.

## > Meeting of the Schengen Information System II supervision coordination group, Brussels

The first Schengen Information System II (SIS II) supervision coordination meeting took place on the afternoon of 11 June 2013. The agenda dealt with administrative matters such as the election of a Chair and Vice-Chair, in which Ms. Clara Guerra representing Portugal's DPA and Mr. David Cauchi representing Malta's DPA were elected respectively; the adoption of the rules of procedure for the group and the recognition of the observer

status of Bulgaria, Cyprus, Ireland, Romania and the UK. More substantive issues such as the hacking of the Danish N-SIS, the state of play of the SIS II migration process and a SIS II information campaign were discussed. Future steps to be taken by the Commission and EU-LISA regarding the SIS II security policy in particular, and future activities of the supervision coordination group for 2013-2014 were also addressed. The next meeting of the group is likely to be in the Autumn.

## SPEECHES AND PUBLICATIONS

- "A clear Signal for Stronger EU Data Protection", editorial (pdf) by Peter Hustinx in "Zeitschrift für Datenschutz", nr. 2013/7, p. 301-302 (21 June 2013)
- "The Stockholm Programme: State of play regarding police and judicial cooperation in civil and criminal matters", speech (pdf) delivered by Peter Hustinx at the Inter-Parliamentary Committee Meeting, European Parliament, Brussels (20 June 2013)
- "Data Protection and Competition: interfaces and interaction", speech (pdf) delivered by Peter Hustinx at a Seminar organised by Covington & Burling LLP, Brussels (13 June 2013)
- "The Increasing Horizontal Impact of Personal Data Protection", editorial (pdf) of Peter Hustinx in 'eucrim' - The European Criminal Law Associations´ Forum, nr 2013/1, p. 1 - Focus: Information and Data Protection. (13 May 2013)

## DATA PROTECTION OFFICERS

☞ 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;
- cooperate with similar authorities to ensure consistent data protection.

☞ **You can subscribe / unsubscribe to this newsletter via our website**



**Follow us on Twitter: @EU_EDPS**

CONTACTS

www.edps.europa.eu
Tel: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50
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

**EDPS – The European guardian of data protection**