EDPS Newsletter

NO36 | FEBRUARY 2013

EUROPEAN DATA PROTECTION SUPERVISOR

- HIGHLIGHTS -

> Inventory of legislative consultations for 2013

On 18 January 2013, the EDPS set out priorities for the year ahead in the area of **legislative consultation** by publishing a strategic planning document, the Inventory. In this document, we have identified issues and areas of **strategic importance** that will form the cornerstone of our consultation work for 2013.

"We live in a technically-mediated world that is constantly evolving. The visibility and relevance of data protection is, thus, greater than ever. The need to take account of the privacy and data protection implications of legislative proposals is becoming essential in all areas of EU policy and leads to an influx of new policy areas for us to deal with. It is becoming increasingly apparent that the fundamental right to data protection cannot be regulated only in data protection law, but that many other different policy areas have to take data protection into account."

Peter Hustinx, EDPS

Our central mission in the field of consultation is to give advice on three main areas: the **revision of the legal framework for data protection, technological developments and the Digital Agenda and further developing the Area of Freedom, Security and Justice.** In addition, we have identified financial sector reform and eHealth as areas of strategic importance for 2013.

Also, in order to better fulfil our advisory role, we will consider publishing so-called *prospective opinions* on important technical or societal phenomena (such as cloud computing) which will highlight their inherent challenges and suggest solutions as appropriate.

☞ EDPS Press release (pdf) and Inventory (pdf)

> EDPS: Status of DPOs is key to safeguarding data protection rights

On 17 December 2012, the EDPS published a report on the status of data protection officers (DPOs) as part of our ongoing task to monitor the compliance of EU institutions and bodies with Article 24 of the EU Data Protection Regulation, which obliges the appointment of DPOs.

> ***"Ensuring the fundamental right to data protection of staff and citizens requires the commitment of the hierarchy within EU institutions and bodies. This can be clearly demonstrated by the appointment and support of their DPOs and also by the status that DPOs hold within the organisation."*** ***Giovanni Buttarelli, Assistant EDPS***

The results of our survey indicate that the DPO function is well established within the EU administration, for example, the experience of the DPO network, the administrative attachment of the majority of the DPOs to the head of the institution or body and the existence of significant staff support for many DPOs.

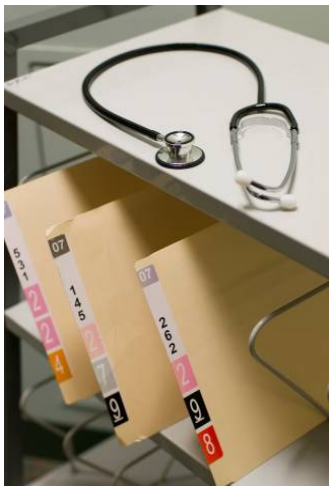
However, there are several areas of concern which we outlined in our report. Under Article 24 of the Data Protection Regulation, individuals fulfilling the DPO position must be appointed for a minimum two year period. But we noted a high turnover of DPO staff and in some cases, shorter mandate terms both possibly linked to the contract status of the staff appointed to this position. In addition, we noted possible conflicts of interest for those combining DPO tasks with other responsibilities and sometimes a lack of adequate resources for DPOs to perform their functions.

As institutions are fully accountable for compliance with data protection rules, it is imperative that these concerns are addressed properly by the institutions and we intend to closely monitor and make recommendations as necessary.

☞ EDPS Press release (pdf) and Report (pdf)

CONSULTATION

> Medical device rules display healthy respect for personal data but need to be more robust



The proposed Commission regulations on medical devices and in-vitro medical devices foresee the processing and storage of large amounts of personal information, potentially saving sensitive data such as patient health information in a European central database (Eudamed).

In our Opinion of 8 February 2013, we recognised and welcomed the specific attention paid to data protection in the proposed regulations. However, we see the need for further improvement and clarification, for example, on the types of categories of personal information to be processed, particularly where sensitive health data might be processed and stored. We recommended that the proposed regulations specify the circumstances under which personal health data may be included in the Eudamed database and that the safeguards for such processing and storage also be outlined.

☞ EDPS Opinion (pdf)

> Preparation to overhaul rules on drug precursors should include data protection in the mix

On 18 January 2012, we published an Opinion on the Commission proposals for amending the regulations on intra-EU trade and on trade with third countries on drug precursors. We welcomed the references in the proposals to the applicability of EU data protection legislation, that many of the categories of information to be processed were specified and that the principle of purpose limitation was mentioned in the external trade proposal.

However, we recommended that the main legislative texts outline all essential elements of the processing operations, such as the exclusion of the processing of sensitive data. In addition, all the categories of information to be processed should be specified at the very least by delegated acts but preferably also in the proposals.

Our other recommendations include:

- that the intra-EU trade proposal specifies that personal information on suspicious transactions may only be used for the purpose of preventing the diversion of scheduled substances;
- the laying down of maximum retention periods for all processing operations;
- appropriate safeguards for international transfers of personal information;
- clarification on who has access to the new European database on drug precursors;
- ensuring the coordinated supervision of the European database by the EDPS and national data protection authorities, similar to that foreseen for the Internal Market Information System;

- prohibiting the interconnection of the European database with other databases created for different purposes.

☞ EDPS Opinion (pdf)

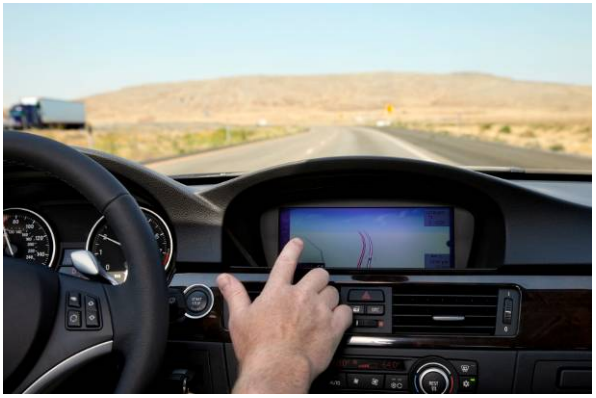
> Clinical trial proposal needs a data protection boost

On 19 December 2012, we adopted an Opinion on the Commission proposal for clinical trials on medicinal products for human use. We were pleased that specific attention was paid to data protection in the proposed regulation, but identified that there was room for improvement.

We recommended that the proposed regulation explicitly refer to the processing of personal information concerning health; clarify whether personal information concerning health is to be processed in the EU databases for clinical trials, and if so, for what purpose; refer to the right of individuals to block their personal information and introduce a maximum retention period for the storage of personal information.

☞ EDPS Opinion (pdf)

> Data protection measures make eCall a smart service



eCall is a system that provides an automated message to the emergency services following a road crash which includes the precise crash location. The in-vehicle eCall is an emergency call (an E112 wireless call) generated either manually by the vehicle occupants by pushing a button or automatically via activation of in-vehicle sensors after a crash.

On 19 December 2012, we published formal comments on a delegated regulation supplementing the ITS Directive 2010/40/EU to harmonise the provision for an interoperable EU-wide eCall. The delegated regulation, adopted by the Commission on 26 November 2012, defines the specifications for the necessary upgrading of the Public Safety Answering Point (PSAP) infrastructure.

We welcomed the several references to data protection law in the text, especially those that define rules on data protection and privacy which make PSAPs and other relevant actors accountable to national data protection authorities for the processing of personal information. We noted with satisfaction that PSAPs (and appropriate emergency services or service partners) put in place the following safeguards:

- no constant tracking of the vehicles equipped with eCall in-vehicle equipment;
- protection against misuse or loss of any data;
- the definition of appropriate modalities for the data storage and processing;
- limiting access to information about the vehicle stored in national databases or elsewhere to when it is appropriate and in accordance with national law and an indication of the types of information that may be accessed.

We were also pleased to note that Member States must inform the Commission about the privacy and data protection protocols that have been put in place in the framework of this delegated regulation.

☞ EDPS Comments (pdf)

> Balancing privacy and transparency in the funding of European political parties and foundations

In our Opinion of 13 December 2012 on the statute and funding of European political parties and foundations, we took the opportunity to reiterate that the role of privacy and data protection is not to prevent public access to information whenever personal information is involved or to unduly limit transparency. Privacy and data protection should ensure that personal information is published only when it is justified and the different interests of those involved have been balanced.

One of the main data protection concerns on this proposal related to making information about the donations and contributions to European political parties and foundations public. We acknowledged that the aim of increasing transparency and trust in the democratic process is legitimate. However, we advised that publishing a threshold for donations and contributions, as recommended in the court case ruling of *Schecke*, would help to achieve the right balance. A justification for such a threshold should also be shown.

☞ EDPS Opinion (pdf)

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.

> EEAS demonstrates willingness to cooperate

On 1 February 2013, we published our first prior-check Opinion on an European External Action Service (EEAS) processing operation. This prior check related to security investigations carried out by the EEAS Division for Security and Security Policy. The original EEAS notification covered various security measures, which we clarified and limited in scope.

In our conclusions, we recommended an amendment of the proposed draft decision on security policy. The EEAS has already confirmed that it will be modified. Another recommendation related to transfers of data - as an external service, this could include transfers to third countries and international organisations - and we referred to our forthcoming paper on data transfers.

☞ EDPS Opinion (pdf)

> When electronic communications should be prior checked...

The EDPS was consulted on the call monitoring data of the unified communication system (UniComm) at the European Union Agency for Fundamental Rights (FRA). In the resulting consultation that we adopted on 1 February 2013, we took the opportunity to clarify those electronic communications cases under which prior-checking notifications are required.

In principle, we consider that electronic communications (and in particular the processing of telephone records) are subject to prior checking under three conditions:

(1) if there is a breach of confidentiality of communication or
(2) the processing relates to suspected offences or security measures or
(3) it is intended to evaluate personal aspects relating to indviduals.

In this case, it appeared that the personal information in question is processed only to ensure the good functioning, identification and handling of security threats against the Unicomm system. Similarly, the processing does not appear to violate the confidentiality of communications, as certain traffic information is processed solely to allow individuals to identify their private calls with no interference to the content of their communications. We concluded, therefore, that the processing operations were not subject to prior-checking.

☞ EDPS Consultation (pdf)

> A fruitful visit to Frontex

As part of our supervisory role, we organised a visit to the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (Frontex) in December 2012. A visit is a compliance tool whose purpose is to engage the commitment of the senior management of an EU institution or agency to foster compliance with the data protection regulation. There are several reasons why we might visit an institution or agency and in this instance, we were concerned by the lack of cooperation between Frontex and the EDPS.

The visit comprised a meeting between the Assistant EDPS and the Executive Director of Frontex as well as meetings with the data protection officer and those in charge of processing operations. We also presented our approach to monitoring and ensuring regulatory compliance in the EU institutions.

The visit proved to be a very useful preliminary assessment of the state of compliance with Regulation (EC) No 45/2001 at Frontex and an excellent opportunity to raise the profile of data protection within the agency.

> EDPS: DPCs play a significant role in supporting DPOs

In recent years, some of the larger EU institutions have established networks of data protection coordinators (DPCs) to act as a relay for the data protection officer (DPO) locally. In June 2012, the EDPS launched a survey relating to the status of DPCs and the mechanisms put in place by the Directorates-General (DG) of the European Commission to comply with Regulation (EC) No 45/2001. In January 2013, we issued a general report of the conclusions from that survey.

The findings of the survey reveal a great disparity between the resources allocated to the function by the DGs, for example, between 5% and 100% of a DPC's time is assigned to the DPC function. However, all DPCs have a common series of basic tasks which they are required to perform irrespective of the time available to do so. One of our conclusions, therefore, is the need to establish minimum criteria for DGs to preserve the useful nature of the DPC role.

Our report also commends some of the good practices developed in certain DGs, such as creating a dedicated mailbox to consult the DPC, developing an intranet page devoted to data protection, making sure the role of DPC is visible in the organisational chart or structuring the DPC's access to his superiors to ensure that s/he is kept informed effectively.

Furthermore, we highlighted in our report that the function of DPC is an element of the current data protection reform: the relation between the DPC role and accountability of the DG on the one hand and the DPC's duty to document processing operations on the other, plays a significant part in supporting the DPO function.

☞ EDPS Report (pdf)

EVENTS

> Belgian DPA publishes recommendation on security measures preventing data breaches

A number of data breaches reported in the Belgian media in early January, prompted the Belgian Data Protection Authority (DPA) to prepare a recommendation on security measures to prevent similar security incidents. The premise of the document is to raise awareness on information security and highlight some fundamental elements to help organisations lay the foundation for an adequate security policy.

Two basic conditions for a successful security policy are management responsibility and employee information. Management must take the initiative to develop a security policy and communicate it fully to employees. A well-documented security policy, supported by all members of the organisation, is key. On a practical level, the Belgian DPA recommends:

- layered security, i.e. different access levels for different areas in the network and logical and/or physical barriers between those areas;
- vulnerability analyses, backed up by an intrusion prevention and detection system.

☞ For more information, read the recommendation which can be found on the Belgian DPA's website in French and Dutch.

> EU binding corporate rules and APEC cross-border privacy rules

The 21 countries of the Asia-Pacific Economic Cooperation (APEC), which include the United States, Canada, Japan, China, Russia, South Korea and Australia, have recently developed a system for cross-border privacy rules (CBPR) to protect privacy and guarantee data transfers.

The CBPR are similar to the binding corporate rules (BCR) that apply to European data transfers. For example, both apply to international transfers developed by companies and are reviewed, a priori, by data protection authorities or by authorised third parties.

As a consequence, the Article 29 Working Party (WP29) decided that work towards a dual 'certification' for CBPR-BCR compliance procedures should be undertaken.

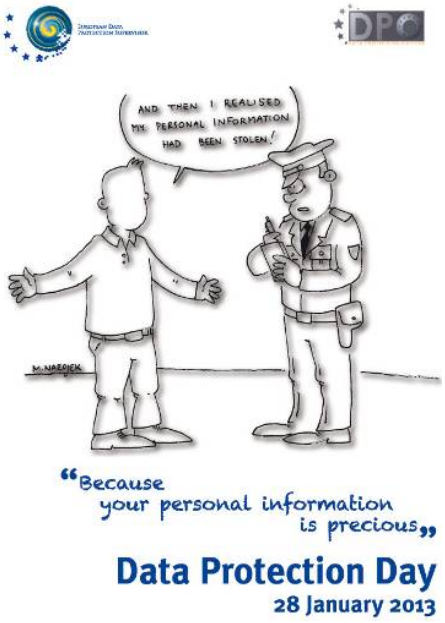
To this end, in late January, representatives of the CNIL, the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), the EDPS and the European Commission met in Jakarta for the first time with the BCR Committee and CBPR APEC members to share their views on the project.

This fruitful meeting resulted in an agreement to develop tools that could be used by multinational corporations that operate both in the EU and the APEC region. A roadmap is likely to be adopted in the coming months by members of the WP29 and APEC to continue this co-operation and realise such tools

☞ Press release issued by the CNIL

> 28 January: Data Protection Day

On 28 January 2013, 47 countries of the Council of Europe as well as European institutions, agencies and bodies celebrated the seventh European Data Protection Day. This date marks the anniversary of the Council of Europe Convention 108 on the protection of personal information, the first legally binding international instrument related to the field of data protection.



This annual event was once again an opportunity for the EDPS and Data Protection Officers from EU institutions to focus on raising awareness among EU staff and others on their data protection rights and obligations. These rights and obligations are set out in the EU Data Protection Regulation and their implementation within the EU administration is supervised by the EDPS.

As part of our awareness raising efforts, we put together a short film as an entertaining and informative way to highlight some of the data protection rights and risks that are inherent in our everyday lives.

To further commemorate the day, in cooperation with the European Parliament (EP), we organised a joint conference *What will the data protection reform change for EU officials and citizens?* The conference was a huge success with standing room only remaining within minutes of the welcome address by EP Secretary-General, Klaus Welle. Following short presentations, Peter Hustinx, Supervisor, Giovanni Buttarelli, Assistant Supervisor and Mr. Paul De Hert, Professor at the Vrije Universiteit Brussels took part in a panel discussion.

We also co-sponsored *A look inside*, an original art exhibition centred on privacy and surveillance with the Vrije Universiteit Brussel and The Privacy Commission of Belgium. Shown at De Markten in Brussels, the exhibition presented the work of young European artists, who used their artistic expression to provoke debate on privacy and its relevance in modern day life.

☞ Speech of Peter Hustinx at the reception of the Privacy Art Exhibition, 28.01.2013

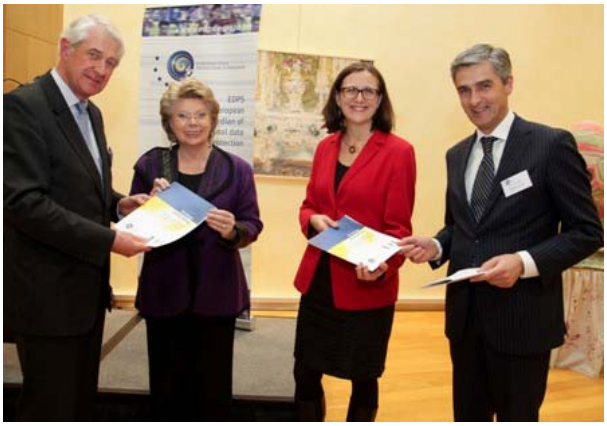
☞ EDPS video message on the occasion of Data Protection Day 2013

Every year the CPDP gathers policy makers, academics, computer scientists, consultants, practitioners and activists from all over the world to exchange ideas and discuss emerging issues in information technology, privacy, data protection and law. This year's conference was entitled Computers, Privacy and Data Protection (CPDP) 2013: Reloading Data Protection. It was a forum to discuss pertinent topics such as cyberwar, internet freedom and the introduction of drones in EU civilian airspace. The conference also featured key debates surrounding the proposed data protection regulation. Several EDPS colleagues took part in panel discussions. Giovanni Buttarelli spoke about the proposed data protection regulation in the opening panel, while Peter Hustinx delivered the closing remarks of the conference.

☞ CPDP website

> Presentation of the EDPS Strategy for 2013-2014

On 22 January 2013, the EDPS presented a report outlining our **Strategy for 2013-2014** to senior representatives of the EU institutions. Both Supervisors and the Director, as members of the Management Board, outlined the process, aims and results of an extensive analysis, including the main lines of the 2013-2014 strategy. This was followed by remarks from Commission Vice-President **Viviane Reding**, Commissioner **Cecilia Malmström**, Parliament Vice-Chair of the LIBE Committee **Sophie in't Veld** and the Council Anti-Terrorism Coordinator, **Gilles de Kerchove**.



Our strategy is based on a strategic review that began in July 2011. The aim of the review was to identify priorities and respond to the **increasing workload** and **broader scope of activities** that the EDPS will face in the coming years. Using our expertise, authority and formal powers, we aim to continue building **awareness** of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions. Acting **selectively** and **proportionately**, we want to ensure that data protection will be an integral part of policy-making and legislation, in all areas where the EU has competence.

In particular, we have identified activities that emphasise the **accountability** of policy makers and data controllers and activities that build on the crucial role of **DPOs**. These activities are key parts of the proposed legislative reforms and will show how levels of compliance can be raised in a period of budget restraint.

We will continue to develop and build on our strategy to respond effectively to the challenge of **achieving excellence in data protection** at European level beyond 2014.

☞ Strategy 2013-2014
☞ Press release Strategy 2013-2014
☞ Video: Highlights of the presentation of the EDPS Strategy 2013-2014

> Workshop on the proposed Data Protection Regulation Warsaw, 12 December 2012

The Assistant Supervisor, Giovanni Buttarelli, and EDPS colleagues took part in a workshop organised by the Polish DPA to debate the effects of the proposed data protection regulation with Polish officials.

A number of questions and concerns were raised about the impact of the proposed regulation on domestic issues and some highlighted the need for improving the proposal. Issues such as the collection of personal information for statistical purposes and the limitations that the proposal puts on such collection, the impact on the processing of personal information by national courts, the lack of clarity on the right to a judicial remedy, the processing of data on children were some of the subjects discussed.

There is a general fear at national level that some provisions in the proposed regulation could lead to the need to change existing sector specific laws that currently provide well-working solutions, for example, Polish labour law contains a limitation restricting the processing of data by employers.

Our conclusions from this very productive workshop were twofold: there is a need for more dialogue with member states (and national administrations) to discuss the correlation between the proposed regulation and national laws which leaves room for maintaining national laws in specific sectors.

Furthermore, the proposed regulation could be further improved on the scope of its application on courts, the definition of the household exemption, the harmonisation of the forum rules for data protection with other types of claims, the rules on statistics to allow recognition of current specific sector rules defined at national level.

SPEECHES AND PUBLICATIONS

- "Privacy moet automatisme zijn", interview of Peter Hustinx (pdf) , De Tijd (22 February 2013)
- "The role of data protection legislation", (pdf) written contribution of Peter Hustinx to the Conference on "Security of e-Government", European Parliament, Brussels (19 February 2013)
- "A Look Inside", (pdf) speech of Peter Hustinx given during the reception at the Exhibition hosted together with the Free University of Brussels (VUB) and the Belgian Data Protection Authority (CBPL-CPVP), Brussels (28 January 2013)
- "Presentation of the Reports on the draft General Data Protection Regulation and on the draft Directive on the processing of data for the purposes of prevention, investigation, detection or

prosecution of criminal offences", (pdf) speaking notes of Giovanni Buttarelli, Meeting of the Committee on Civil Liberties, Justice and Home Affairs, European Parliament, Brussels (10 January 2013)

- "EU Data Protection Law - Current State and Future Perspectives", (pdf) speech of Peter Hustinx given at the High Level Conference: "Ethical Dimensions of Data Protection and Privacy", Centre for Ethics, University of Tartu / Data Protection Inspectorate, Tallinn (9 January 2013).

DATA PROTECTION OFFICERS

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

☞ 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