ISSN: 1977-9127

European Data Protection Supervisor

EDPS Newsletter

No. 41 | April 2014

IN THIS ISSUE

HIGHLIGHTS

A single set of rules for all: EU Data Protection Reform can support businesses and protect citizens

The reform of the EU rules on data protection will support the recovering but still fragile European economy, said the European Data Protection Supervisor following the presentation of his Annual Report of activities for 2013 to the Committee on Civil Liberties, Justice and Home Affairs (LIBE) at the European Parliament. The reformed rules should provide for clarity and consistency throughout Europe: the same rules will apply to all firms who do business in the EU, regardless of where they are based, and citizens will be more confident of how their personal information is treated.

The European Parliament has voted resoundingly in favour of the reform package which will offer a uniform set of rules that will make it simpler - and more economical - for online and traditional businesses to follow. The onus is now on the Council to support the package, guaranteeing citizens the right to control what their personal information is used for and the right to recourse if they are unfairly targeted or discriminated against.

Peter Hustinx, EDPS

EDPS Annual Report 2013

EDPS Press Release

Enforcing EU data protection law essential for rebuilding trust between EU-US

The strict enforcement of existing European data protection laws is an essential element for restoring trust between the EU and the USA, said the European Data Protection Supervisor (EDPS) following the publication of his Opinion on 20 February 2014.

The rights of EU citizens to the protection of their privacy and personal information are enshrined in EU law. The mass surveillance of EU citizens by US and other intelligence agencies disregards these rights. As well as supporting a privacy act in the USA, Europe must insist on the strict enforcement of existing EU legislation, promote international privacy standards and swiftly adopt the reform of the EU data protection Regulation. A concerted effort to restore trust is required.

Peter Hustinx, EDPS

EDPS Opinion

EDPS Press Release

Active supervision by the EDPS effective in keeping EU bodies on track for data protection

EU institutions are better at complying with data protection rules and privacy principles than ever before. This is the overall message of the EDPS report, published on 27 January 2014, on his latest general stocktaking exercise.

I'm delighted with the progress that the EU institutions have made. 10 years of our active supervision have resulted in significantly higher levels of compliance with data protection obligations across EU services.

This is a powerful indication that institutions are recognising that they are accountable for applying data protection rules.

Peter Hustinx, EDPS

EDPS Report

EDPS Press Release

SUPERVISION

Human error results in security breach

On 27 November 2013, the EDPS was made aware of an apparent breach of Regulation EC No 45/2001 involving the disclosure of candidates' e-mail addresses following a recruitment application process at an EU agency. It transpired that an HR assistant sent out an e-mail to inform 205 non-selected candidates that they had not been successful in their applications for a specific post. In this particular case, a manual mistake was made by an assistant in the HR team who, instead of blind copying all the addresses in the 'BCC' field of the email, accidentally included them in the 'TO' field. We were satisfied that the agency had adequate preventative measures in place at the time of the incident, to minimise any risk to personal data. A number of further measures have been (or will be) implemented following the incident, to mitigate the risk of any other disclosures. We recognised that this particular data breach was caused by a manual error, which did not seem to have occurred as a result of any negligence on the agency's part in terms of data security.

EDPS Consultation

The new Regulations for EU officials & the further processing of staff evaluations

The new *Staff Regulations* for EU officials provide for some changes to the annual evaluation procedure or career development review (CDR). The Regulations state that one unsatisfactory CDR should result in blocking the biannual advancement in step, three consecutive ones in downgrading and five consecutive ones in dismissal of the person concerned.

The data protection officer (*DPO*) of the Commission informed the EDPS about the first further use of the CDR as soon as the corresponding general implementing rules were adopted.

In our letter of 28 January 2014, we insisted that the persons concerned are *informed* about the further or additional purpose of processing information collected for annual evaluations, as well as about the right of appeal.

As Article 110 of the new Staff Regulations provides for the applicability in principle of the general implementing rules of the Commission to all 44 agencies, the EDPS decided to share its recommendations in this case with all DPOs in order to provide the necessary guidance in this matter.

EDPS Letter

ARACHNE: no data protection cobweb

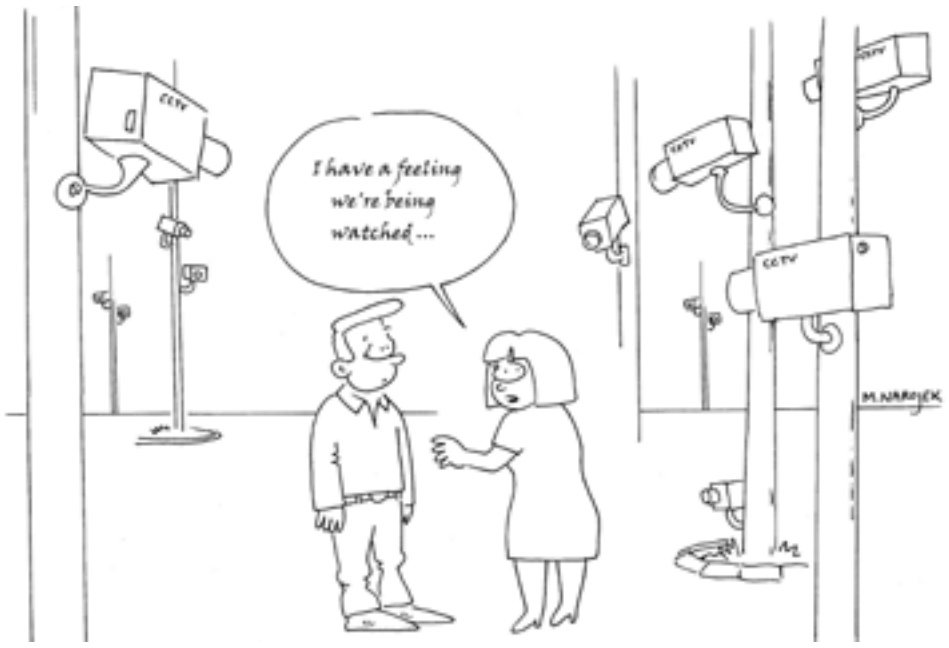
ARACHNE, a risk-analysis system, is part of the European Commission's fraud prevention and detection strategy in the area of Structural Funds (European Social Fund and European Regional Development Fund). It complements an existing database with publicly available information in order to identify the most risky projects based on a set of risk indicators, which are used to help auditors in identifying and selecting future candidates for audit. Unlike other processing operations with the purpose of fraud detection, ARACHNE does not endeavour to assess the individual conduct of fund recipients or exclude beneficiaries from the funds.

The recommendations in our Opinion of 17 February 2014 refer, among other things, to the need to ensure data quality and the information to data subjects. Given that ARACHNE will, for example, contain information on individuals to whom sanctions are applied, we expressed a preference for the adoption of a more specific legal basis authorising the processing of special categories of personal data under Article 10(5) of the Regulation.

EDPS Opinion

Video-surveillance: EDPS welcomes improvements in EU bodies

Based on our 2010 *Video-Surveillance Guidelines*, and as announced in our 2012 *Follow-up Report*, the EDPS conducted targeted inspections at 13 Brussels-based institutions and bodies in 2012 and four similar inspections in Luxembourg in 2013. These focussed on the way in which information about video-surveillance is provided to the general public. The inspection report for the inspections in Luxembourg was issued on 13 January 2014. Under Regulation 45/2001, EU institutions and bodies are accountable, in other words, responsible for ensuring compliance and for demonstrating compliance to their supervisory authority, the EDPS. The positive results of these recent inspections indicate that our advice has been implemented - a successful example of EU institutions and bodies applying the principle of accountability.



EDPS Press Release

EDPS Factsheet on CCTV

CONSULTATION

Progress on the data protection reform package

Under the Greek presidency, discussions on the proposed General Data Protection Regulation (GDPR) are continuing in the Council. In a letter sent to the President of the Council of the European Union on 14 February, we set out our views on **three crucial points** of the reform which remain unresolved.

Firstly, we stressed the need to ensure that **the public sector remains within the scope of the GDPR**. Indeed, providing for a broad exception, as apparently advocated by some member states, would constitute a step back from current data protection *acquis*, given that neither the Data Protection Directive 95/46/EC nor the Council of Europe Convention 108 make a distinction between public and private sector. More importantly, many activities such as the provision of health care services, may be performed by either public or private entities that should be subject to the same set of rules.

We also weighed in on the hotly debated issue of the **one-stop-shop**, stressing the importance of this principle in the proposed harmonisation of the data protection framework. In our view, the one-stop-shop principle does not unduly restrict the rights of the data subjects to an effective judicial remedy and to a fair trial and can indeed be reconciled with a high standard of protection for citizens' fundamental rights, including those protected by Article 47 of the Charter of Fundamental Rights.

In conclusion, we commented on the **principle of accountability** and the 'risk-based approach', stressing the particular need for clear criteria according to which a risk assessment should be performed, in order to direct compliance efforts towards areas where they are needed most.

Payments in the internal market

On 5 December 2013, we issued an Opinion on the legislative package for *payment services in the internal market and interchange fees for card based payment transactions*. The Directive aims to give consumers a series of new rights while an accompanying Regulation will cap the fees retailers pay to banks to process debit and credit card payments and should also reduce the costs to consumers. In our Opinion, we welcomed the introduction of a substantive provision that stated that any processing of personal data taking place in the framework of the proposed Directive should be done with full respect to the national laws implementing Directive 95/46/EC and Directive 2002/58/EC, and of Regulation EC No 45/2001.

We recommended that references to applicable data protection law should be specified with concrete safeguards that will apply to any situation in which personal data processing is envisaged and it should be expressly clarified that the processing of personal information may only be carried out to the extent necessary for the performance of payment services. We also highlighted other data protection issues, for example in the exchanges of information, third party access to account information and security reporting.

EDPS Opinion

Disruption of illegal traffic of firearms should target data protection

In our Opinion of 17 February 2014 on the Commission communication on *firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking*, we highlighted the data protection requirements that apply, particularly to the priorities and tasks outlined in the communication.

We insisted on the importance of addressing these issues at an early stage of the legislative process, possibly during the stakeholders' consultation, and on including in every regulatory text a reference to the applicable data protection legislation.

More specifically, we raised the data protection issues relating to:

- the marking of firearms;
- the eventual requirement of medical and criminal checks as a condition for the lawful purchase and ownership of any firearm;
- the installation of biometric sensors on firearms; and
- the sharing of information between law enforcement and customs authorities, particularly through large-scale IT systems.

EDPS Opinion

Data-matching to combat cross-border social security fraud needs data protection safeguards

The Commission requested the EDPS to provide preliminary comments on a possible proposal under consideration for amending the Regulation on the *coordination of social security systems* which aims to improve procedures controlling cross-border social security fraud - particularly in the exchange of information between member states.

Data matching is a process whereby two sets of personal data are matched in order to identify any information which is inconsistent. For instance, one member state provides death data to the home country of individuals so that it can cross check it against its own records of pensions (or other allowances) being paid to those residing in the other member state.

In our comments of 17 January 2014, we welcomed the intention to modify the current legal framework to provide more clarity on the exchange of bulk data in the form of 'data-matching'. In addition to insisting on the necessity and proportionality of any data-matching practice, we highlighted that it is particularly important to:

- ensure transparency about what data-matching consists of;
- ensure that there should be no automatic denial of benefits based on the results of the data-matching procedure; and
- guarantee fair procedures for individuals to contest any decisions that were taken on the basis of automatic matching procedures.

EDPS Comments

Protecting personal data in the agri-food chain

A new Regulation on *official controls and other official activities performed to ensure the application of food and feed law* is currently being discussed by the European Parliament and Council. The proposal envisages the processing of two general sets of data, namely data related to operators, such as individual or company's names, place of establishment, websites, ratings etc. and data related to the operators' assets, such as animals and goods. It also outlines the exchange of information between national competent authorities via an EU wide IT network, the IMSOC.

In our comments of 20 February 2014, we clarified that:

- data concerning goods and animals could *relate to* an *identified or identifiable* individual operator, thus falling within the concept of 'personal data';
- data protection rules apply to the processing of data envisaged by the Regulation in so far as data relates to an operator who runs his business as a natural person, or the official title of the legal person identifies one or more natural persons, or other information about legal persons may be also considered as 'relating to' natural persons, or if the national laws, including those implementing Directive No 95/46/EC at domestic level, extend the protection of personal data to legal persons as well;
- IMSOC shall implement the concept of privacy by design and by default and the Commission shall bear the responsibility of its controllership for the exchange of personal data within the system, including providing data subjects with a first 'layer' of data protection notice and other relevant information on its multilingual website, also 'on behalf of' competent authorities.

EDPS Comments

Internet engineers discuss improvement of privacy and security

The Internet Engineering Task Force (IETF) is the not-for-profit organisation that develops and promotes internet standards, in particular for the internet protocol suite (TCP/IP etc.). At the IETF meeting in London in early March this year, internet engineers followed up on the results of their previous meeting in Vancouver last November (see our report in the December 2013 issue of the EDPS *newsletter*), where they had agreed to consider mass surveillance of internet communications as a threat and that this threat, as any other, should be countered with technical measures. The IETF meeting in London featured workshops on privacy and discussions about the best way to engineer privacy into the very fabric of the internet, through its protocols. The IETF meeting was preceded by a dedicated *workshop* of more than a hundred IT specialists who discussed over 60 papers on ways to strengthen the internet against pervasive monitoring.

The first priority for many engineers is to make effective use of properly implemented cryptographic tools (low-level coded algorithms that are frequently used to build computer security systems) in order to increase the security of networks and communications. Privacy experts have already pointed out that other privacy principles, such as data minimisation, anonymisation and aggregation should also be considered in technical design. Finding useful technical solutions to implement these principles is a task that will continue to require broad cooperation. The EDPS is proposing an *initiative* for bridging the communications gap between privacy experts and engineers and bring them together to work on technical tools for enhanced privacy in internet tools and applications and invites expressions of interest by internet developers.

Will mobile security be the key challenge for privacy?

Mobile communication capabilities are becoming the main driver in the interconnected world. More and more devices are equipped with Wi-Fi, bluetooth, 4G or other interfaces that allow direct connection to the internet or via smart phones or home networks. Wearable devices such as sports monitors equipped with satellite navigation technology record biometric data, the location and movement of their user and transmit them to the servers of their manufacturers as soon as they are connected. Household appliances can communicate with local networks and cars can record and transmit data about their functions, position and behaviour of their drivers.

Internet giants are investing significantly in mobile and embedded technologies: several companies providing mobile messaging, home automation or robotics have been acquired recently. In addition, they are investing heavily in research and development for mobility e.g. in autonomous cars.

While these trends are likely to increase the collection and transmission of personal data over the networks, there are concerns that security might not be keeping up. The number of serious security flaws discovered in widespread systems is increasing as well. A recently fixed *programming error* had made some of the most popular mobile devices vulnerable to man-in-the-middle attacks which would enable the attacker to intercept seemingly encrypted communications. Shortly after that incident, a problem with open-source software was also detected. A piece of code found in many linux systems had a *critical flaw* that would allow attackers to bypass some transport layer security (TLS) protections. This means that programs using the affected packages are vulnerable to attacks that may allow decoding of encrypted communications. In both cases, software updates fixing the bugs have since been made available. Another vulnerability was recently discovered in a smartphone using an android operation system, where the chip responsible for the communication over the network could override all restrictions protecting the 'smart' part of the phone, and so gain access to all information stored on the smartphone. Anyone who could get control of the communications module could use this *backdoor* into the users' phone. A solution has been developed for this specific configuration, but it may not reach all affected phones quickly.

While the software of most computers and many mobile devices is frequently updated so that they have installed versions without the known vulnerabilities, this is much less certain for other devices with embedded communications capabilities, such as TV sets or household appliances. For such devices, the provision of software updates often ends shortly after their sale, long before the end of their usual lifetime. Vulnerabilities of their 'old' operating systems and functions remain in place and can serve as an entry for attackers, who rely on well-known weaknesses in old software versions. Even some of the routers which provide the network access have been found to contain such weaknesses.

This situation constitutes a huge challenge for manufacturers, distributors and service providers that aim to build the Internet of Things, or the internet of everything. Devices must be developed in a way that is secure and have the ability to remain secure through periodic operational updates. Without a solution for this problem, the roll-out of connected devices could be seriously inhibited by justified security concerns.

EDPS lab to open in spring

In 2013, in order to increase our technology monitoring capabilities and to assess the privacy features of certain products or systems used in the field of our supervision work, the EDPS initiated plans to build an IT laboratory. The lab will help us to assess the privacy effects of new technical developments in mobile device communications and to inspect the data protection compliance of websites. The EDPS IT lab should become operational in spring 2014.

The lab may also be used for testing new or modified platforms with data protection relevance, such as results of university research projects or new industry products.

In future, we may offer IT graduates following our traineeship programme or post-graduate laureates that spend part of their research period at the EDPS the use of our lab facilities for research and development projects. The lab would allow them to pursue some technical R&D and conduct experiments.

In view of this potential, we are more actively promoting the EDPS *traineeship programme* to those studying informatics and related subjects who are also interested in exploring the technological aspects of data protection and privacy. The EDPS offers a paid traineeship of five months for university graduates as well as the option of unpaid internships for post-graduates who already receive support from other programmes and would like to pursue specific research tasks in Brussels.

DATA PROTECTION OFFICERS

SPEECHES AND PUBLICATIONS

- Speech (*pdf*) delivered by Peter Hustinx in Brussels, "Opportunities and challenges in the digital era: big data and moral hazard" (1 April 2014)
- Speech (*pdf*) delivered by Peter Hustinx in Brussels, "EDPS Comments on the Data Protection Supervision of Europol" (12 February 2014)
- Speech (*pdf*) delivered by Peter Hustinx in Bonn, "Change of Office: Farewell Celebration and Inauguration" (4 February 2014)
- Speech (*pdf*) delivered by Peter Hustinx in Bonn, "The European single market proposal for the electronic communication sector as an area of tension between data protection, net neutrality and economic freedom" (13 January 2014)

About this newsletter

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

- monitor the EU administration's processing of personal data;
- give advice on data protection legislation;
- cooperate with similar authorities to ensure consistent data protection.

You can subscribe / unsubscribe to this newsletter via our website.

CONTACTS

www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
NewsletterEDPS@edps.europa.eu

POSTAL ADDRESS

EDPS
Rue Wiertz 60 – MTS Building
B-1047 Brussels
BELGIUM

OFFICE ADDRESS

Rue Montoyer 30
B-1000 Brussels
BELGIUM

Follow us on Twitter: @EU_EDPS

EDPS - The European guardian of data protection

QT-AC-14-001-EN-C