ISSN: 1977-9127

European Data Protection Supervisor

EDPS Newsletter

No. 44 | February 2015

IN THIS ISSUE

HIGHLIGHTS

2015-2019 EDPS Strategic Plan

Big data, big data protection

Advances in technology are bringing untold benefits and opportunities, but it is important to ensure that these benefits do not come at the expense of our fundamental rights. With Data Protection at the top of the EU and international agendas, the new European Data Protection Supervisor, Giovanni Buttarelli, is dedicated to developing innovative and future-oriented solutions to these emerging challenges.

Congratulations to dynamic new EDPS team

Institutions and high level representatives from across the world, including outgoing European Data Protection Supervisor (EDPS) Peter Hustinx, have offered their congratulations to the new team of Supervisors at the EDPS. Former Assistant EDPS, Giovanni Buttarelli, was appointed as the new European Data Protection Supervisor by a joint decision of the European Parliament and the Council on 4 December 2014, while Wojciech Wiewiórowski replaces Mr. Buttarelli as Assistant Supervisor.

"We are entering a crucial phase for European data protection. The rapid development of new technologies demands appropriate solutions. I am committed to supporting the EU legislator fully in its work to ensure that the data protection reform is adopted in 2015 and that modern and forward-thinking data protection mechanisms are implemented. In confronting the issues associated with big data, the time has come to make privacy and data protection more effective in the digital environment."

Giovanni Buttarelli, EDPS

"I am looking forward to building on my experience in effective enforcement and technological know-how in order to make existing and new data protection principles more effective in practice. EU institutions need to ensure a high level of compliance and further implement the principle of accountability that will be developed in the reform."

Wojciech Wiewiórowski, Assistant Supervisor

SUPERVISION

EDPS Guidelines on conflicts of interest: data protection strengthens good public administration

In December 2014, the European Data Protection Supervisor published Guidelines on the collection and publication of Personal Data with regard to the management of conflicts of interest in EU institutions and bodies. In these Guidelines, the EDPS encourages *EU institutions and bodies* (EU institutions) to balance transparency in the interests of the public and

the data protection rights of individuals when managing the declarations of the conflicts of interest of people working for them. This balancing exercise can strengthen their efforts to foster the trust of the public as well as those who work for them.

By taking data protection fully into account, EU institutions can ensure openness and transparency and better manage declarations of interests in a fair way, demonstrating the independence of those working for them as well as exercising a duty of care towards them.

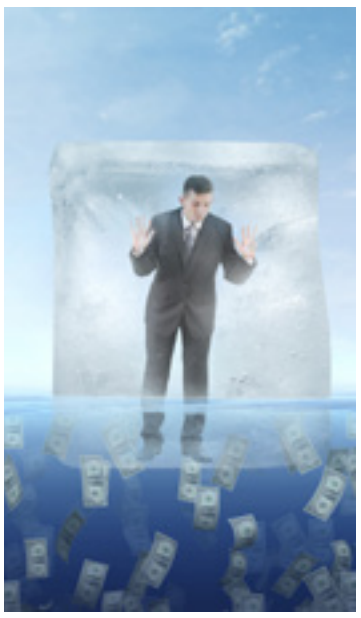
Giovanni Buttarelli, EDPS

EDPS Guidelines

Council's cold response to problems with asset freezing

An asset freezing measure adopted under Article 215 of the *Treaty on the Functioning of the European Union* (TFEU) led to complaints from several people affected by it. Their complaints concerned the processing of their personal data by the Council of the European Union.

The complainants successfully challenged their inclusion on the Council's asset freezing list in Court and were subsequently delisted. However, the Council failed to take any further steps to publicly clear the names of the people affected, as recommended by the EDPS, in several *Opinions*.



The original publication of the names of the complainants as persons subject to asset freezing in the Official Journal of the EU, cannot be revoked. However, the EDPS did find that the complainants are entitled under Article 16 of the Data Protection Regulation to the deletion of any of their personal data which has been processed by the Council, and that the Council should take additional measures to publicly clear the complainants' names. This might include explaining the reasons why the complainants were de-listed in the amending act, which is published in the Official Journal, or detailing these reasons in a letter to the person concerned.

Technical error leads to data protection breach

In spring 2014, a technical error led one European institution to publish personal information about its staff on its website. The information, which was collected for internal purposes and meant for publication on the institution's internal network, included job descriptions, first names and, in some cases, photos. One member of staff complained about this breach, which the EDPS investigated.

We concluded that a breach of Article 22 of the Data Protection Regulation had occurred in this case. However, we also concluded that the institution responded to the breach in a satisfactory manner and had taken the necessary measures to prevent a similar breach from recurring in the future.

A hands-on approach to increasing compliance

During November 2014, a member of the EDPS Supervision and Enforcement team completed a secondment period at the European Satellite Centre (EU SatCen). This took place as part of a pilot project organised by the EDPS to facilitate exchanges, visits and short secondments. The objective of the secondment was to promote a data protection culture in EU SatCen and provide the agency with practical guidance on how to reach full compliance with Regulation (EC) 45/2001.

The experience was considered a success by both parties. Working with an EDPS staff member, those responsible for the processing of personal data at EU SatCen were able to successfully file notifications of *data processing* operations according to their procedures, set out relevant data protection safeguards and, in doing so, develop a greater awareness of data protection principles. For the EDPS, the experience proved an interesting challenge in how to ensure a good level of data protection compliance within a very short period of time. It was also very useful to witness first-hand the practical implementation of EDPS Guidelines.

Following the positive results of this pilot project, the EDPS now hopes to facilitate future secondments and exchanges, aimed at achieving similar levels of success and improvement in standards of data protection compliance across the EU institutions and bodies.

Whistleblowing made easy and data protection friendly

The European Ombudsman recently drafted its internal rules on whistleblowing. These rules aim to safeguard the rights and interests of whistleblowers and provide adequate remedies if they are not treated correctly and fairly.

It is a legal obligation, laid down by Article 22a of the Staff Regulations and included in the Conditions of Employment of Other Servants of the European Union, for all staff members to report fraud, corruption or other serious professional wrongdoing within the EU institutions and bodies. A whistleblowing procedure exists to facilitate this.

Our Opinion of 4 December 2014, focused on the need to ensure that the data collected by the European Ombudsman from whistleblowing reports are relevant and that the information collected is not excessive taking into account the allegations made. As this requires a very quick response to each whistleblower's report, we recommended that information on how to deal with excessive data should be explicitly detailed in the Ombudsman's internal rules.

In addition to this, we clarified that preserving the confidentiality of whistleblowers, the accused and third parties are of the utmost importance. We also reminded the European Ombudsman that personal data does not only relate to information about an individual's life, but also to information regarding their activities.

EDPS Opinion

CONSULTATION

Balancing privacy and transparency

In 2014, the Commission adopted a *proposal* for amending Directive 2007/36/EC and Directive 2013/34/EU on shareholder engagement and the corporate governance statement. The proposal put forward by the Commission aims to enhance transparency and encourage long-term shareholder engagement.

Particularly relevant for data protection, the proposal gives companies the right to identify their shareholders. It also requires public disclosure of the remuneration packages received by individual directors, published in the remuneration report which shareholders can vote on.

In our Opinion of 28 October 2014, the EDPS recommended that the proposal specify the purpose for which the relevant data will be collected and processed. We also advised the Commission to clearly state that the information collected on the identity of shareholders and on the remuneration packages of individual directors will not be used for any inappropriate or unstated purposes. In addition, the proposal should include a requirement for companies to ensure that technical and organisational measures are put in place to limit access to information on the individuals concerned after a certain period of time. It should also require that relevant information be redacted where the disclosure of details relating to an individual director's remuneration package would lead to the release of more sensitive data, such as health data.

EDPS Opinion

How to make a drone data protection friendly

The *Commission Communication* of 8 April 2014 addresses the civil use of remotely piloted aircraft systems, more commonly known as drones. The civil use of drones involves any use that is not military.

In our Opinion of 26 November 2014, we stressed that the processing of personal data via a drone for commercial or professional purposes must comply with the relevant EU country's national data protection legislation, which is based on Data Protection Directive 95/46/EC. This stipulation also applies to the majority of cases in which drones are used privately by individuals.

Drones might be used by many different organisations or persons for many different purposes. This could include big commercial organisations such as Amazon, but it might also include agricultural companies using drones to monitor crops, or a concert organiser using them to ensure security during an event. Drones might also be used by law enforcement bodies charged with surveying illegal immigration at borders. To ensure that their activities comply with data protection legislation, we underlined that anyone using drones and processing the data collected by them must ensure that they provide the relevant information to any individual whose personal information is involved. They must also ensure that the information they collect is appropriately protected and not stored for any longer than necessary.

In addition to this, we welcomed a number of initiatives and awareness raising projects proposed by the Commission. These projects should be made accessible as soon as the drones themselves are introduced in the EU civil market. We also recommended that the Commission encourage drone manufacturers to employ privacy by design and by default in their design processes.

EDPS Opinion

Speeding towards the safe exchange of data on road traffic offences

The Commission asked the EDPS for comments on a proposal for a Directive to facilitate the cross-border exchange of information on road safety related traffic offences. The proposed Directive will replace Directive 2011/82/EU, which was annulled by the Court of Justice of the European Union due to an incorrect legal basis.

The new Directive represents an almost identical text to the first but with a changed, and correct, legal basis. Considering this change, the Commission consulted us specifically on the question of whether Directive 95/46/EC was the applicable data protection law in this case.

In our comments of 3 October 2014, we welcomed the Commission's citation of Directive 95/46/EC as the relevant data protection law. However, we also emphasised that this is not a clear-cut, simple case. While it is important to refer to Directive 95/46/EC, ensuring that all processing activities respect the obligations set out in Article 8 of the Charter of Fundamental Rights is also essential. These obligations, in turn, must be interpreted in light of more detailed rules on data protection, including those applicable to the police sector, but most notably those set out in Directive 95/46/EC.

EDPS Comments

Assessing the impact on fundamental rights

In the second half of 2014, the European Commission conducted a *public consultation* on new draft Impact Assessment Guidelines, aimed at gaining the views of stakeholders. On 30 December 2014, the EDPS responded to this public consultation.

In our letter to the Commission, we stressed that both the Lisbon Treaty and the Charter of Fundamental Rights, which came into force in 2009, place strong emphasis on the protection of fundamental rights in the EU, and in particular the rights to privacy and the protection of personal data.

Recent judgments from the Court of Justice, such as the annulment of the EU Data Retention Directive in the *Digital Rights Ireland* case and the right to request removal of certain information from search engines in the *Google Spain* case, reinforce this, confirming the need for EU activities to uphold the fundamental right to privacy and data protection. It is, therefore, imperative that the Commission takes all the necessary steps, starting from the earliest stage of the EU decision-making process, to ensure that these rights are respected.

In our comments, we made several specific suggestions about how this could best be achieved, such as by providing more precise guidance and examples for Commission policy makers on how to ensure that policy remains in line with the Charter.

EDPS Comments

ipen initiative keeps growing

The EDPS' Internet Privacy Engineering Network (*IPEN*) initiative recently featured as the subject of panel discussions at both the *IAPP Congress* in November 2014 and the *CPDP conference* in January 2015. In addition, a recent *report* by ENISA provided an overview of current approaches to privacy design and engineering techniques, referring to IPEN and offering valuable input for the work of the initiative. Following the success of the initiative's first *workshop* in September 2014, IPEN continues to grow, with informal meetings and phone conferences providing forums for discussion.

The work of IPEN is now entering a new phase in which our focus will turn to ensuring that progress is made on the ten action items agreed upon by participants at the IPEN workshop in September 2014. This will involve setting up communications infrastructures, such as repositories, and consolidating the IPEN mailing lists and a *website* in order to most effectively organise IPEN's resources. While initiators have been identified for all action items, there is still space for new volunteers to join our effort to increase the standard of privacy engineering on the Internet.

The next major milestone for the IPEN initiative will be a stock-taking of achievements. This will take place at a second IPEN workshop to be scheduled for the summer of 2015.

Intelligent transport systems require intelligent approach to privacy

On 3 November 2014, the EDPS took part in a kick-off meeting of the working group on Governance and Privacy, focused on the European Commission's Cooperative Intelligent Transport Systems (C-ITS) *Platform*. C-ITS consists of a group of technologies and applications that allow vehicles to connect to one other and to other elements of the transport system, such as traffic control or toll collection systems. The aim of this information exchange is to help avoid collisions and contribute to road safety as well as to improve and optimise traffic movements. The working group comprises experts from national authorities and the Commission as well as from public and private organisations active in C-ITS, such as automobile clubs, car manufacturers, toll road operators and manufacturers of navigation systems and other car electronics.

The working group on Governance and Privacy is to provide recommendations on data protection and privacy issues for the development and deployment of C-ITS in the EU. Privacy is a significant concern in the deployment of C-ITS due to the capability it has to collect huge amounts of data, such as location, vehicle model and identification number and driving speed, as well as the personal information of C-ITS users including their name, address or driving licence number. This information, when linked together, could be used to conduct user profiling or tracking.

In our presentation to the working group, we built on our previous work in this field, such as the EDPS opinions and comments on *eCall*, *digital tachographs* and *Intelligent Transport Systems (ITS)*. We pointed out that it is crucial to clarify the roles of the different actors involved in ITS in order to identify who is responsible for ensuring that data protection principles are upheld. We also underlined the importance of considering privacy and data protection from an early stage of the ITS systems design process (privacy by design) and the need to take appropriate security measures to protect personal information from unauthorised access, loss, misuse, modification and disclosure.

Personal data lost in translation

On 5 December 2014, the EDPS gave a presentation at a *conference* on machine translation at the European Commission. Our presentation concerned the terms and conditions of free internet translation services, a considerable number of which are available online and widely used. However, while these services may not cost you money, you pay for them with your personal data.

Translation services keep translated texts in their corpus to further develop and improve their capabilities, meaning that a record of anything you type into them will be saved and stored by the translation service as soon as you click 'translate'.

When these services are used in a professional context, it is essential that attention is paid to data protection and security issues. Users must apply caution so as not to disclose personal data to the translation services or any other third parties without appropriate safeguards. This is even more important when we consider that these third parties might be located in non-EU countries with inadequate data protection standards. There is also always the risk that uncontrolled use of free translation services in a professional context may disclose the internal information of an organisation to unintended recipients.

It became clear at the conference that EU translation services are aware of these risks, and that the security and confidentiality of texts is treated as one of the driving objectives for the development of in-house machine translation services.

Biometrics: how secure are they?

The process of authenticating a person's identity is based on something a person knows, such as a password; something a person has, such as a badge or key card; or something physical about that person, their biometrics.

Biometrics include fingerprints, voice tone, hand geometry and other individual characteristics and play a fundamental role in strong, multifactor authentication systems, used to protect important assets, such as *information* or *money* - both of which the EDPS has analysed in detail in past Opinions.

Biometric authentication has several advantages over other forms of authentication, principally that your biometrics are always with you and that you cannot forget them. However, this advantage is also a weakness, as a recent *press report* made clear.

Biometrics are not secret: your voice can be easily recorded and your fingerprints can easily be stolen by someone with the right tools. Moreover, unlike a password, you cannot simply change your biometrics if they are compromised. As a consequence, the benefits of biometric systems can only be realised when stringent safeguards are applied. This could include basing biometric systems on technologies which are particularly difficult to steal or copy, or combining biometrics with other forms of identification.

European Data Protection Day 28 January 2015

Everyday personal information is collected, shared, used and stored by individuals, organisations and public authorities. Recruitment activities, video surveillance and health data collection are just a few examples of this.

On 28 January 2015, 47 countries of the Council of Europe as well as European institutions, agencies and bodies celebrated the ninth annual 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.

Data Protection Day is an opportunity for the EDPS, along with Data Protection Officers from the EU institutions, to raise awareness among EU staff and the general public 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.

This year, the EDPS marked Data Protection Day with a range of events. This included our lunchtime conference Personal Information – Smarten Up! in which representatives from the EDPS outlined the risks to personal data and how to better protect your data on smart devices such as phones. Those interested can watch the event online on the *EDPS website*. For more information, please contact: *EDPS-Events@edps.europa.eu*

DATA PROTECTION OFFICERS

Recent appointments

- Ms. Vanesa Hernandez Guerrero, European Research Council Executive Agency (ERCEA)
- Ms. Anne Salaün, ECSEL
- Ms. Sophie Vuarlot-Dignac, European Securities and Markets Authority (ESMA)

French and German versions of this newsletter will be online shortly.

8TH INTERNATIONAL CONFERENCE
21 22 23 JANUARY 2015 • BRUSSELS BELGIUM
COMPUTERS, PRIVACY & DATA PROTECTION
DATA PROTECTION ON THE MOVE
WWW.CPDPCONFERENCES.ORG

CPDP offers the cutting edge in legal, regulatory, academic and technological development in privacy and data protection. Within an atmosphere of independence and mutual respect, CPDP gathers academics, lawyers, practitioners, policy-makers, computer scientists and civil society from all over the world to exchange ideas and discuss the latest emerging issues and trends.

This unique multidisciplinary formula has served to make CPDP one of the leading data protection and privacy conferences in Europe and around the world. Organised with the support of the EDPS, this year's panels focused on key issues that cover all current debates: the data protection reform in the EU: European and Global developments; mobility (mobile technologies, wearable technologies, border surveillance); EU-US developments concerning the regulation of government surveillance; e-health; love and lust in the digital age; internet governance and privacy; and much, much more, including a closing address from new European Data Protection Supervisor, Giovanni Buttarelli.

For more information: *cpdpconferences.org*

You can also follow CPDP on Facebook (*CPDPconferencesBrussels*) and Twitter (*@cpdpconferences*).

SPEECHES AND PUBLICATIONS

- 'Speech (*PDF*) delivered by Giovanni Buttarelli in Brussels during the Joint debate at the extraordinary meeting of the LIBE Committee in the European Parliament "Counter-Terrorism, De-Radicalisation and Foreign Fighters" (27 January 2015)
- 'Speech (*PDF*) delivered by Giovanni Buttarelli in Brussels at the 8th CPDP Conference "Computers, Privacy & Data Protection - 2015 Data Protection on the Move" (23 January 2015)
- 'Speech (*PDF*) delivered by Giovanni Buttarelli in Brussels at the European Parliament's Privacy Platform "Privacy and Competition in the Digital Economy", (21 January 2015)'
- "Big data, big challenges", article (*PDF*) by Giovanni Buttarelli for New Europe (5 January 2015)
- Speech (*PDF*) delivered by Wojciech Wiewiórowski in Krakow "European and international cooperation in enforcing privacy - expectations and solutions for a reinforced cooperation", (12 December 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-14-004-EN-C doi:10.2804/62844 ISBN 978-92-95076-45-7