ISSN: 1977-9127

EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS NEWSLETTER

No. 46 | December 2015

IN THIS ISSUE

HIGHLIGHTS

EDPS encourages a new debate on Big Data

On 19 November 2015, as the European Data Protection Supervisor (EDPS) published his *Opinion*, *Meeting the Challenges of Big Data*, he said he wanted to launch a new, open discussion with *legislators*, *regulators*, *industry*, *IT experts*, *academics and civil society* to explore how the social benefits that big data brings can be harnessed while better protecting the dignity and the fundamental rights and freedoms of individuals in a more effective and innovative way.

> ***Big data implies bigger data protection and more user control is key for its responsible application in the future. Privacy laws have been developed to protect our fundamental rights and values. The question industry and public entities must ask themselves is not whether to apply these laws to big data processes, rather how to apply them more effectively. We want to engage with all key interlocutors, in and outside the EU, to explore creative and future-oriented solutions to better preserve values while achieving social benefits in the public interest.***
>
> Giovanni Buttarelli, EDPS

EDPS Opinion

EDPS Press Release

A collaborative approach to data protection reform

Twice a year, a network of over 60 *Data Protection Officers* (DPOs) from all EU institutions, bodies and agencies meets to exchange ideas and experiences relating to good practice in data protection. The most recent edition, organised in November by the European Union Agency for Network and Information Security (ENISA) in Athens, provided an opportunity to prepare for the upcoming data protection reform.

Specifically, the meeting gave us an opportunity to discuss the new mechanisms which will be used to enforce compliance with data protection rules, such as data protection impact assessment, *accountability* and *privacy by design* and by default.

Building on the interactive approach we established at the *DPO meeting in Luxembourg* earlier in 2015, the EDPS once again played the role of facilitator, organising a number of workshops on issues such as how to put data protection principles into practice and the handling of complaints.

Each EU institution or body is legally obliged to appoint a DPO, whose job it is to develop a data protection culture within their institution and make data protection part of the day-to-day EU administration. Their experience on the ground is not only an increasingly valuable asset to the EDPS, in our role as advisor to the EU institutions, but also to their fellow DPOs, who can learn from the experiences of others and apply them in their own work. The ability to work together in this way will prove especially valuable as we move towards the reform, allowing us to ensure that the EU institutions and bodies continue to set the standard in data protection and privacy.

Towards a new digital ethics: Data, Dignity and Technology

As the European Data Protection Supervisor (EDPS) published his *Opinion*, *Towards a New Digital Ethics*, on 11 September 2015, he urged the EU and also those responsible internationally, to promote an ethical dimension in future technologies to retain the value of human dignity and prevent individuals being reduced to mere *data subjects*. He said that his independent institution will soon set up an external Ethics Group that will help to better assess the ethical implications of how personal information is defined and used in the big data and artificial intelligence driven world.

> ***The future technological environment will be made up of an interdependent ecosystem of legislators, corporations, IT developers and individuals. Each should be equally responsible for shaping it and any imbalance of power risks its sustainability. For example, the continued, massive and indiscriminate collection of personal information by governments and businesses risks killing the golden goose. With this Opinion, which complements our Opinion on the EU Data Protection Reform, we want to launch a broader discussion, both in the EU and globally, on how to ensure the integrity of our values while embracing the benefits of new technologies.***
>
> Giovanni Buttarelli, EDPS

EDPS Opinion

EDPS Press Release

SUPERVISION

EDPS examines recruitment complaint

The EDPS recently handled a complaint relating to a request for access to personal data in a recruitment procedure at an EU body; the complaint concerned access to written feedback on the complainant's performance during the recruitment process.

In our *Guidelines* on the Rights of Individuals with regard to the Processing of Personal Data the EDPS recommends that *qualitative comments*, used to justify marks given in the recruitment process, should be made available to those individuals concerned who request them.

Whilst the EU body in question had provided the complainant with their marks for each evaluation section of the recruitment procedure, it failed to provide them with the reasons for these marks. The EU body claimed that this information had been made available orally and that providing these qualitative comments in writing would endanger the secrecy of the selection board proceedings.

As outlined in our Guidelines, the secrecy of the selection board's discussions is one of the reasons for which access to these comments can be denied.

However, in this case, we judged this argument invalid. In making its comments available orally, the EU body had already decided that their availability was not compromising the secrecy of the selection board's discussions and therefore could not rely on this argument to justify their refusal to provide the comments in writing.

The EU body subsequently complied with our decision and provided the complainant with a paper copy of the comments requested.

Supervision and enforcement in action

All *EU institutions* are obliged to comply with their data protection *obligations* and to be able to demonstrate this compliance to their supervising data protection authority, the EDPS. In turn, we are very active in our supervision and enforcement role and we reserve the right to inspect all EU institutions and bodies, not only those which deal with a lot of *personal data* or where we have identified shortcomings.

Between 9 and 11 June 2015, we inspected the EU Translation Centre in Luxembourg. This inspection is an example of our commitment to data protection compliance across the board as, unlike many EU institutions, the core business activities of the Translation Centre do not involve the processing of personal data.

The data processing activities of the Translation Centre relate only to its role as an employer. Our inspection therefore focused on the processing of personal data in staff selection, staff evaluation, public procurement and the management of freelance translators. We also followed-up on the implementation of the relevant recommendations outlined in *EDPS Guidelines*, making it clear that implementing these recommendations is integral to ensuring compliance.

In our supervisory capacity, the EDPS will continue to carry out inspections in our effort to ensure that all EU institutions and bodies comply with EU data protection rules. We will communicate the results of our inspection to the Translation Centre later this year.

Commission demonstrates data protection compliance

In early 2015, we inspected the Directorate General for Human Resources (DG HR) at the European Commission. Inspections are opportunities for institutions to demonstrate their compliance with data protection *rules* and are therefore a valuable tool for the EDPS to check and enforce this compliance.

This inspection was significant as DG HR is a large organisation, responsible for processing personal information related to selection and recruitment within the DG and also for advising other Commission DGs on how to integrate data protection principles into their recruitment activities.

Our inspection, therefore, focused on the selection processes used by DG HR, specifically on how personal information is handled, the right of individuals to access their data and the physical, electronic and organisational security of this data.

We checked whether the *personal data* processed in recruitment activities is relevant and necessary, particularly in the case of criminal records and birth certificates; we also verified that DG HR had implemented our previous recommendations on the right of Commission staff to access the electronic personnel files of staff members who have moved to other institutions.

While we concluded that DG HR is compliant with relevant data protection rules, we also outlined some recommendations for improvement. As with all other inspections, we will follow up on this case until all recommendations have been implemented, applying increasingly forceful measures if necessary. In this way we ensure that data protection rules are adequately implemented across all EU institutions and bodies.

CONSULTATION

A further step towards comprehensive EU data protection: EDPS recommendations for the police and justice sectors

The reform of the EU data protection rules is more urgent than ever, said the European Data Protection Supervisor (EDPS), following the publication of his *Opinion* on the proposed Directive for data protection in the police and justice sectors on 28 October 2015.

In the Opinion on the Directive, the EDPS recalls that data protection in the police and justice sectors should be fully consistent with the general rules contained in the General Data Protection Regulation (GDPR) and should only contain specifications and adjustments where necessary in view of the specific nature of these sectors. The scope of the Directive should be limited to the areas where specific rules are really necessary, namely the activities of criminal law enforcement by police and judicial authorities, as was the case in the original proposal of the Commission. Moreover, the performance of law enforcement tasks by non-public entities and organisations should be subject to the GDPR.

The Opinion on the Directive follows the publication on 27 July 2015 of the *EDPS recommendations on the GDPR*, both in the form of an Opinion and an app. The EDPS will release an update of this *EU Data Protection app* in the coming weeks, to include specific recommendations from the EDPS on the proposed Directive.

EDPS Opinion

EDPS Press Release

EU PNR: EDPS warns against unjustified and massive collection of passenger data

On 24 September 2015, as the EDPS published his Second *Opinion* on the use of *Passenger Name Records (PNR) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, he said that there is a lack of information to justify the necessity of an EU PNR scheme.

Europe is facing serious terrorist threats and we fully recognise the need for appropriate action. As an independent institution, we are not a priori in favour of or against any measure. However, according to the available information, no elements reasonably substantiate the need for the default collection of massive amounts of the personal information of millions of travellers. Necessity and proportionality are essential prerequisites for the legitimacy of any intrusive measure. We encourage the legislators, in assessing the necessity of such a measure, to further explore the effectiveness of new investigative approaches as well as of more selective and less intrusive surveillance measures based on targeted categories of flights, passengers or countries.

Giovanni Buttarelli, EDPS

EDPS Opinion

EDPS Press Release

EDPS statement on latest developments on EU PNR

Increased tax transparency, decreased data protection

On 8 July 2015, the EDPS published an *Opinion* on the EU-Switzerland agreement on the automatic exchange of tax information. The Opinion came in response to the EU's adoption, on 27 May 2015, of an amending protocol to the Savings Agreement, an agreement between the European Community and the Swiss Confederation in the area of tax cooperation.

The new agreement aims to regulate the exchange of financial, tax-relevant information between governments in the EU and Switzerland, putting an end to banking secrecy in tax matters. The new agreement will harmonise EU relations with Switzerland in line with EU and international developments in this area, through the use of the *automatic exchange of information*.

However, though the agreement represents an important step in the fight against tax evasion, the data protection provisions included in the agreement do not go far enough.

In our Opinion, we outline five specific recommendations which should be taken into account in the negotiation of future bilateral agreements in this area and which should be introduced in any updated versions of agreements that have already been finalised. These recommendations include making the collection and exchange of tax-relevant information conditional on the risk of tax evasion, only processing data in pursuit of a legitimate policy goal and specifying an explicit retention period for the tax information exchanged.

EDPS Opinion

COURT MATTERS

EU Court declares safe harbour agreement invalid

On 6 October 2015, the Court of Justice of the European Union (CJEU) *declared* the European Commission's *safe harbour decision* invalid. The Court's decision followed the *opinion* of Advocate General Bot, given on 23 September 2015. It argued that, due to the threat of US mass surveillance, personal data transferred to the US under the arrangement was not adequately protected. The transfer of personal data through this process is therefore illegal.

The safe harbour arrangement was negotiated by the Commission more than 15 years ago to ensure that personal data transferred from the EU to the US received the same level of protection as it would in the EU. Though it was not the only way to transfer data between the two, it was widely used. Many large American technology companies transferred data on the basis of this arrangement, including Facebook; the court ruling concerned a complaint by Austrian citizen Max Schrems, related to transfers of personal data by Facebook Ireland Ltd. to the servers of its US parent company, Facebook Inc. (see *EDPS Newsletter 45*).

In its judgment, the Court clarified that, when negotiating *adequacy decisions* such as safe harbour, the Commission is obliged to assess both the content of the data protection rules in the country in question and the measures designed to enforce compliance with these rules. This assessment should be repeated on a regular basis to ensure that the rules in place continue to provide for a level of data protection which is *essentially equivalent* to the one that exists in the EU.

Additionally, the Court ruled that national *data protection authorities* (DPAs) have the authority to examine complaints relating to the enforcement of the Commission's adequacy decisions. National DPAs can therefore investigate the level of protection provided by an adequacy decision and challenge its validity on behalf of any individual who raises concerns.

The Article 29 Working Party, of which the EDPS is a member, responded to the ruling in a *press statement*, released on 16 October. The statement clarified the judgment's key points and highlighted the urgency of developing a new approach to the transfer of data to the US, which adequately respects the fundamental rights of EU citizens. Until this new approach is finalised, companies will have to rely on other means of transferring personal data to the US, such as *standard contractual clauses* or *binding corporate rules*.

Judgment

WP29 Press Release

Defining establishment

On 1 October 2015, the Court of Justice of the European Union (CJEU) *ruled* on the case of *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*. The ruling clarifies the powers of a national *data protection authority* (DPA) in relation to a company operating, but not registered in, the DPA's jurisdiction and ensures that all EU citizens are able to exercise control over their data and how it is used, regardless of the country they live in.

In accordance with EU law, each EU member state is required to adopt its own national data protection law based on the provisions outlined in the *EU Data Protection Directive*. They are also required to appoint a national DPA with powers to enforce this law within their national territory. The national data protection law applicable to a specific company, and thus the national DPA with the power to enforce this law, depends on where the company is deemed to be *established*.

Weltimmo is a company registered in Slovakia which runs a property dealing website for Hungarian users. These users complained to the Hungarian DPA after the company refused to erase their accounts. However, it was not clear whether Hungarian data protection law or Slovakian data protection law applied to the case, nor if the Hungarian DPA would be able to enforce Slovakian law should that be required. The case was therefore referred to the CJEU.

The Court's decision centred on the notion of *establishment*, which it said should be interpreted flexibly. *Establishment* therefore not only refers to the country in which a company is registered, but also to countries in which a company carries out a real and effective activity - even a minimal one - by means of *stable arrangements*. Even the presence of one representative can, in some circumstances, be sufficient to fulfil this criterion. Consequently, Weltimmo is considered to be *established* in Hungary and therefore subject to Hungarian data protection law.

The Court also ruled that, irrespective of the national law applicable, a DPA must evaluate all claims addressed to it. In particular, the powers of a DPA to impose fines can only be exercised in compliance with the principle of territorial sovereignty and therefore not outside the jurisdiction of the Member State. Consequently, a DPA cannot impose penalties on the basis of the applicable law of another member state, but should request the DPA of the relevant member state to act, in accordance with relevant provisions of the Data Protection Directive. The requirement to inform individuals is all the more important since it allows them to exercise their rights of access to, and right to rectify, their personal data, and the right to object to the processing of their data.

These decisions reinforce the fundamental right of all EU citizens to data protection and privacy throughout the EU by ensuring that all companies are subject to the data protection laws of the countries in which they operate and therefore accountable to each individual to which they offer a service.

Judgment

Transfer request denied: Court clarifies transfer rules

The Court of Justice of the EU (CJEU) released its *decision* on 1 October 2015 in a case relating to the transfer of personal information. The decision reinforces the right of the individual to be informed of when and where their personal data is being processed by national governments and public bodies by clarifying the exceptions to this rule.

The case concerned the transfer of personal data from Romania's national tax authority to its national health insurance authority, which was carried out without informing the individuals concerned.

EU data protection law obligates those involved in the processing or transferring of data to inform the individuals concerned that these actions are taking place. In its judgment, the CJEU held that this obligation to inform individuals follows from the basic requirement of fair processing set out in Article 6 of the Data Protection Directive.

The only circumstances under which personal data can be transferred and processed without informing the individuals concerned is when the transfer is laid down in law which has been made public, and only to the extent the processing of the personal data at stake are necessary to comply with that law.

The decision provides for increased transparency in the actions of national governments and public bodies, ensuring that the right to be informed that our data is being processed is consistently upheld.

Judgment

Transparency and data protection: a balancing act

In July 2015, the Court of Justice of the EU (CJEU) ruled on two cases related to transparency and data protection. The judgments provide some clarity on how to reconcile the need for transparency and openness in the *EU bodies* with the fundamental right to data protection.

EU citizens have the right to request access to documents from EU public bodies in the interest of transparency and openness. However, EU institutions and bodies have an obligation to protect the personal data of individuals which might appear in these documents. It is, therefore, important to clarify under which circumstances the protection of personal data should prevail.

In the case of *Dennekamp v. European Parliament*, the Court found that the right to information and the right to freedom of expression were not sufficient reasons to warrant the transfer of personal data of Members of the European Parliament (MEPs) to a journalist. The possibility of uncovering conflicts of interest, however, was considered sufficient. *Supported* by the EDPS, Mr. Dennekamp had argued that the public interest in transparency warranted access to information about MEPs affiliated to a now defunct pension scheme.

In the case of *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA)*, in which the EDPS also *intervened*, the Court ruled that the identity of external experts who had commented on a draft guidance document produced by EFSA should be made available, on the basis that increased transparency demonstrates the impartiality of the experts in question. It was considered that this kind of transparency in EU decision making was necessary to ensure that EU bodies remained accountable to the citizens they serve.

Under *EU data protection rules*, access to personal data can only be given when it can be shown that the transfer of personal data meets the criteria of necessity and proportionality and provided that the individual's legitimate interests are not prejudiced by the disclosure. The cases give an insight into the arguments which meet these criteria and the arguments that do not, allowing us to further define and understand the relationship between data protection and transparency.

Judgment Dennekamp v. European Parliament

Judgment ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA)

IT POLICY

Encryption: security threat or protector of privacy?

The use of encryption for economic and social purposes was the subject of Assistant EDPS Wojciech Wiewiórowski's presentation at the *Free and Safe in Cyberspace* conference, which took place in Brussels on 24-25 of September 2015.

Following recent terrorist attacks in Europe and the ongoing discussion on government surveillance, some law enforcement and political representatives have called for restrictions on encryption, ways to break it or the weakening of encryption tools for consumers.

The risks of such an approach for the economy and society at large are significant and have already been analysed and discussed in the past; the integrity of encryption has been recognised as necessary for the digital economy and for the protection of fundamental rights, such as privacy and free speech.

European organisations have always criticised other regimes who implemented the kinds of measures now being proposed in the EU. The *Council of Europe*, the *European Parliament* and the *European Commission* have all defended the right to and need for encryption to protect personal data.

While law enforcement requires the means to fight crime on the internet, any new measure would have to pass the test for necessity and proportionality in advance, based on substantiated evidence. While encryption makes bulk data collection and mass surveillance difficult, it is not a limiting factor in more targeted and specific measures.

The recent data breach of the company Hacking Team, which produces dedicated intrusion and surveillance tools, and the subsequent leak of a significant amount of *their information* on the internet, has shown that law enforcement authorities are already using tools that enable them to covertly monitor individuals. These tools, which should also be subjected to a thorough analysis of necessity and proportionality, are not hindered by encryption, thus undermining the argument that law enforcement needs to be able to break encryption mechanisms in order to be effective.

As the recently adopted *report* by MEP Marietje Schaake states, encryption is *an important method that helps to secure communications and the people using them*. In doing so, it preserves the fundamental right of all EU citizens to data protection and privacy.

INTRODUCTION TO ENCRYPTION

Encryption is used to ensure that information is hidden from anyone for whom it is not intended. Decryption is the process of reverting encrypted information to its original form. Cryptography is the science of using mathematics to encrypt and decrypt data.

In symmetric encryption, one key is used both for encryption and decryption. For a sender and recipient to communicate securely, they must agree upon a key and keep it secret. If they are in different physical locations, they must use a "secure" communication medium otherwise they risk disclosing the secret key during transmission. Anyone who intercepts the key can read, modify, and forge all information encrypted or authenticated with that key.

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. While the public key is published, the private key is kept secret. Anyone with a copy of the public key can then encrypt information, but it will only be readable using the associated private key.

The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely.

International Data Protection

The annual International Conference of Data Protection and Privacy Commissioners took place in Amsterdam from 26-29 October 2015. Hosted by the Dutch Data Protection Authority, the Conference was an opportunity for data protection leaders from across the world to discuss some of the most important issues in data protection and privacy today. The main theme of the conference was *privacy bridges*. Discussion on this topic focused on a *report* prepared by a group of EU and US experts in privacy and data protection. The report identifies 10 practical steps, or *bridges*, that will result in better-informed, and more consistent, regulatory cooperation, policy guidance, and enforcement activity across the world, without any change in the law.

Also discussed were the privacy challenges of genetic data. Due to technological developments, it is likely that genetic data will soon be widely available. As the genetic information of one individual also contains information about their ancestors and descendants, it is essential that we begin to address the personal data protection implications of developments in genetic analysis.

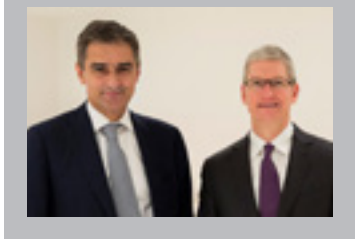
Side events to the conference were an opportunity to exchange ideas on the role of ethics in data protection. Following the *announcement* that the EDPS will appoint an external Ethics Advisory Group in early 2016, EDPS, Giovanni Buttarelli and Assistant Supervisor Wojciech Wiewiorowski participated in a discussion on this topic, where they were able to elaborate and gain feedback on their plans.

Giovanni Buttarelli also participated in the final panel of the conference, which focused on the future of data protection. He was joined on the panel by *several high level experts*. The discussion proved particularly interesting given the recent decision of the Court of Justice of the European Union to suspend the Safe Harbour agreement between the US and the EU.

Four resolutions were adopted at the conference related to the challenges facing data protection and privacy today. All of them can be found on the *EDPS website*. For more information about the Conference, visit the website of the *37th International Privacy Conference*.

EDPS meets Apple CEO

Following his *speech at Bocconi University* on 10 November 2015, Apple CEO Tim Cook met with European Data Protection Supervisor Giovanni Buttarelli. Addressing students and faculty at the Italian business school in Milan, Cook stressed the importance of privacy as a fundamental right.



Rebooting cooperation between digital regulators

On 24 September 2015, the EDPS, in association with the European Academy of Law (ERA), hosted *Competition Rebooted*, a workshop focused on examining the need for closer collaboration between digital regulators and on upholding the interests of individual people in the digital age.

The event brought together economists and legal specialists and included discussions on topics such as the implications of Big Data for society and the current state of cooperation between competition and data protection authorities. Speakers, including representatives from the European Commission's Directorate General for Competition, the UK Competition and Markets Authority and a consumer advocacy association, addressed the relevance of privacy in the assessment of market power and consumer welfare, as well as the need to guard against data breaches, which are an unfortunate inevitability in the digital world.

On 26 March 2014, the EDPS published an *Opinion* on privacy and competitiveness in the age of big data and we plan to publish a further Opinion on antitrust and privacy in the coming months. The Opinion will include specific recommendations for EU action in this area, including setting up a digital market clearing house, designed to coordinate the exchange of information between relevant parties and thus ensure that the European Commission's *Digital Single Market* strategy is implemented in a coordinated manner.

Dealing with data protection at HOME

On 21 September 2015, the EDPS held a joint workshop with the European Commission's Directorate General for Migration and Home Affairs (DG HOME) to discuss the data protection and privacy considerations related to policies in these areas. The workshop was attended by staff from both policy areas who deal with privacy and data protection issues and therefore proved a useful way of reinforcing good data protection practice in the work of the DG.

After an introduction about the differences between the right to privacy and the right to data protection and a general overview of data protection rules and principles, participants split into two parallel break-out sessions. One focused on borders and the other on law enforcement access and the exchange of law enforcement information. In the interactive discussions that followed, we were able to identify possible difficulties related to data protection and privacy in the policy areas concerned and give participants the opportunity to discuss how to address them.

The feedback gathered during the workshop is now being considered as the basis for the development of EDPS guidelines. These could be used by staff at DG HOME to help identify the data protection and privacy implications of their policy proposals.

Buttarelli visits the Bay Area

Shortly after the publication of our *Opinion* on digital ethics, European Data Protection Supervisor Giovanni Buttarelli went on a fact-finding tour of the San Francisco Bay Area and Silicon Valley, the global hub of technology-driven growth and creativity. His aim was to investigate how best to cultivate technological innovation in the EU without compromising the fundamental rights of EU citizens.

He spoke to both large, established companies and to start-ups about emerging capabilities, such as artificial intelligence, autonomous vehicles and peer-to-peer sharing platforms, all of which rely on processing a vast amount of diversely-sourced personal information. He also met with state and federal representatives to discuss how best to regulate these continually developing markets at state and federal level.

This experience in the US has given us an insight into how the EU, as it invests in digital-led growth, might learn from the West Coast experience. In particular, we are dedicated to ensuring that all technology is grounded in respect for human dignity and developed with privacy-conscious engineering which builds data protection and the interests of the individual into the design of products and services. For more details on the tour and our conclusions, you can read our report which will be available soon on the *EDPS website*.

Successful collaboration requires commitment

We stand on the brink of a new European data protection reform that will place new demands on national Data Protection Authorities (DPAs) to work much closer together than we do today. In the future, cross-border matters will be addressed by the European Data Protection Board (EDPB) and assigned for joint handling. Also imminent is the *Global Cross Border Enforcement Cooperation Arrangement*, adopted at the International Data Protection Conference in Mauritius in 2014, which emphasises cooperation and collaboration between DPAs on a global scale.

In May 2012, representatives from the Data Protection Authorities in the Nordic countries met in Oslo, Norway. The main topic of discussion was the EU data protection reform. During the meeting, the Nordic DPAs decided to perform a joint audit of banks with activities in all Nordic countries. The goal of the project was to evaluate the feasibility of joint audits spanning several countries.

The project is now finished and here are some conclusions and recommendations for future joint audits:

Datainspektionen

- Before deciding to go ahead with a project, a budget and a plan specifying man-hours and other resources to be invested must be accepted by all parties involved;
- The project participants should report to a reference group that consists of executives from each DPA;
- It is important that the participants in the project meet in person on at least one occasion, preferably more often. Meeting in person is important for several reasons, not least to build trust between the participants and form a sense of a shared mission;
- The workload between the participating authorities must be evenly distributed so that the project is considered equally important for all the participating authorities;
- Consider carefully what audit method to use.

Joint audits may require well-defined goals, comprehensive project directives and support at the executive level from all involved parties, but, most of all they require real commitment and a will to collaborate. This is mostly new ground for the European DPAs, but ground that we must now all prepare to cover. I look forward to working more closely with all of my European colleagues.

Kristina Svahn Starrsjo, Director General at the Swedish Data Protection Authority

SPEECHES AND PUBLICATIONS

- "The General Data Protection Regulation: Making the world a better place?", keynote speech (*PDF*) given by Giovanni Buttarelli at the at EU Data Protection 2015 Regulation Meets Innovation event, San Francisco, United States (8 December 2015)
- "A Data Protection perspective on the Smart Borders Package - focusing on the possibility of law enforcement authorities' access to border data", speech (*PDF*) given by Giovanni Buttarelli at European Council, the Working Party on FRONTIERS, Brussels, Belgium (19 November 2015)
- "Europe's big data protection opportunity", keynote address (*PDF*) given by Giovanni Buttarelli at the Banking and Payments Federation, Ireland (8 October 2015)
- "Competition Rebooted: Enforcement and personal data in digital markets", keynote speech (*PDF*) given by Giovanni Buttarelli at the Joint ERA-EDPS seminar (24 September 2015)

DATA PROTECTION OFFICERS

Recent appointments

- Silvia Polidori, European Defence Agency

See full list of DPOs

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

© Photos: iStockphoto/EDPS & European Union

EDPS - The European guardian of data protection

QT-AC-15-002-EN-N ISBN 978-92-95073-01-2