ISSN: 1977-9127

EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS NEWSLETTER

No. 49 | October 2016

IN THIS ISSUE

HIGHLIGHTS

SUPERVISION

CONSULTATION

IT POLICY

EVENTS

SPEECHES AND PUBLICATIONS

DATA PROTECTION OFFICERS

HIGHLIGHTS

The coherent enforcement of fundamental rights in the age of big data

The European Data Protection Supervisor (EDPS), Giovanni Buttarelli, has announced that he intends to set up a Digital Clearing House to promote more coherent enforcement of EU rules. In a new *Opinion*, *Coherent enforcement of fundamental rights in the age of big data*, published on 23 September 2016, he drew attention to the mounting concern at concentration of market power and personal data in fewer and fewer hands, with the internet experience characterised by *walled gardens* and take-it-or-leave-it data use policies. This means that authorities need to work more closely to protect the rights and interests of individuals, like the right to privacy, to freedom of expression and non-discrimination.

Data protection, consumer and competition law each in theory serve common goals, but in reality they generally work in silos, according to the EDPS. Each branch of the law has its own role to play, but they will be more effective if they work in tandem. The Digital Clearing House will be a voluntary network of regulators willing to share information and ideas on how to make sure web-based service providers are more accountable for their conduct.

EDPS Opinion

EDPS Press Statement

Migration, security and fundamental rights: A critical challenge for the EU

As the EU searches for the best approach to secure its borders, the European Data Protection Supervisor (EDPS) said that citizens must be assured that the proposals put forward are effective, but that they also respect data protection laws. In his Opinions on the *Common European Asylum System* (CEAS) and the *Smart Borders Package*, he said that it is vital that the reform of the EU's border policy be further assessed to ensure its full consistency with the respect for the fundamental rights of those who enter and leave the EU.

Giovanni Buttarelli, EDPS, said: ***"The EDPS understands the need for the EU to better address the challenges of migration, borders and refugees. However, we recommend considering additional improvements in the revised proposals which will involve a significant collection of data concerning non-EU nationals whose freedoms, rights and legitimate interests may be significantly affected. Border management and law enforcement are distinct objectives and need to be more clearly distinguished. Refugees, asylum seekers, illegal immigrants and ordinary travellers may require separate considerations."***

The reforms proposed by the European Commission are designed to fill gaps in the EU's current border management policy and both the CEAS and Smart Borders package also provide for access for law enforcement purposes. While it is important that EU countries strengthen security by stepping up intelligence cooperation and data sharing, the EDPS cautions that Europe's freedoms and fundamental rights are fully respected in practice in the process.

EDPS Opinion on the Common European Asylum System

EDPS Opinion on the Smart Borders Package

EDPS Press Release

Data protection and Whistleblowing in the EU Institutions

Confidentiality is the most effective incentive to encourage staff to report wrongdoing at work said the European Data Protection Supervisor (EDPS) on 18 July as he published his *Guidelines on Whistleblowing Procedures.*

Wojciech Wiewiórowski, Assistant EDPS, said: ***"Whistleblowing procedures are meant to provide safe channels for staff or other informants to report fraud, corruption or other serious wrongdoing in organisations. Given that the information processed in whistleblowing procedures is sensitive and that leaks or unauthorised disclosure may have adverse consequences both for the whistleblowers and the accused, special care must be taken over that information. The EDPS Guidelines can help the EU institutions and bodies to mitigate the risks."***

EDPS Guidelines

EDPS Press Statement

SUPERVISION

Making sure you have a safe flight

Aviation safety is not just about the planes. Pilots also need to be in good health. To ensure this is the case, all commercial pilots undergo regular medical examinations at which they must be certified *fit to fly*.

However, the *Germanwings crash* in 2015 exposed some flaws in the existing system. It is the responsibility of the pilot to inform their doctor if their certificates have ever been suspended or revoked and pilots are entitled to carry out the examination with any qualified doctor in the EU. Rules exist to enable doctors to check the information their patients give them, but it can be hard for doctors to identify if their patient is telling the truth or not and asking all competent national authorities for information about a specific pilot is often impractical.

To solve this problem, the European Aviation Safety Agency (EASA) has proposed the setting up of a database which would allow doctors to easily check whether a pilot's certificate has ever been suspended or revoked and to contact the relevant authorities for further information. The EASA would provide the system, named the European Aeromedical Repository (EAMR), but it would not have access to the data. The final decision on whether a pilot is fit to fly would remain the doctor's responsibility.

In our *Opinion* on the proposal, we outlined the need to ensure that a valid legal basis exists to set-up the database. A new EASA Regulation is currently being debated in the European Parliament and the Council and is likely to include a specific legal basis for such a database. However, this cannot be used by the EASA until the Regulation comes into force. We also recommended that pilots are appropriately informed about the system and that they will be able to access their own data.

EDPS Opinion

Balancing the conflicting rights of victims and harassers

Harassment in the workplace, whether psychological or sexual, is an offence. Those found guilty face disciplinary and even criminal, proceedings. However, when dealing with harassment cases it is important to respect both the confidentiality of the victim and the rights of the alleged harasser.

Most EU institutions have an informal anti-harassment procedure in place and have appointed counsellors to help mediate any conflicts. The EDPS has also issued *Guidelines* on this procedure, which aims to resolve the complaint privately and confidentially. However, if it proves unsuccessful, a formal investigation might be launched.

In this case, the victim's confidentiality must be carefully balanced against the rights of the alleged harasser both to be informed about the accusations they are facing and to have access to their personal information. Simply asking for the victim's consent to share specific data with the alleged harasser is not appropriate. Indeed, in any employment context the use of consent should be avoided as it is impossible to ensure that this consent is being given freely.

Instead, it is the responsibility of the investigators to assess the relevant and necessary information to be shared with the harasser and to inform the victim. They must also make it clear that the victim has the right to object to such communication based on legitimate grounds and that, if disciplinary proceedings are launched, the alleged harasser will be granted broader access to the harassment file in order to exercise their right to a defence.

EDPS Guidelines

CONSULTATION

Commission President highlights importance of data protection

Data protection featured in European Commission President Jean-Claude Junker's *State of the Union Address* in Strasbourg on 14 September 2016.

In his speech, President Juncker focused on both security issues and European values. While he highlighted the importance of defending the EU's borders through the implementation of the new EU border package, he also stressed that information and intelligence exchanges must not interfere with our fundamental values. He made it clear that data protection is a core EU value and a top priority, citing the General Data Protection Regulation as evidence for this.

State of the Union Address 2016

ePrivacy rules should be smarter, clearer, stronger

A new proposal on ePrivacy should guarantee confidentiality of communications, offer clarity and complement the General Data Protection Regulation (GDPR) said the European Data Protection Supervisor (EDPS) as he published his *Opinion* on the review of the ePrivacy Directive.

Giovanni Buttarelli, EDPS, said: ***"The confidentiality of online communications by individuals and businesses is essential for the functioning of modern societies and economies. The EU rules designed to protect privacy in electronic communications need to reflect the world that exists today. By preserving and not reducing the high level of protection offered by the current ePrivacy Directive and harmonising some specific provisions to complement the GDPR, the EU can reinforce the confidentiality and integrity of our electronic communications."***

In his Opinion, the EDPS says that the scope of new ePrivacy rules needs to be broad enough to cover all forms of electronic communications irrespective of network or service used, not only those offered by traditional telephone companies and internet service providers. Individuals must be afforded the same level of protection for all types of communication such as telephone, voice over IP services, mobile phone messaging app, Internet of Things (machine to machine).

EDPS Opinion

EDPS Press Release

New data protection rules come into force

After four years of intense discussion, the General Data Protection Regulation (GDPR) was finally adopted earlier this year.

The GDPR was published in the *Official Journal of the European Union* on 4 May 2016 and will be fully applicable in all EU countries in May 2018. EDPS Giovanni Buttarelli has described the new Regulation as a *landmark in human* rights law while Assistant Supervisor Wojciech Wiewiórowski proclaimed it a victory *for the protection of fundamental* rights in Europe.

The new rules mean new responsibilities for public authorities and private companies, including the appointment of a data

protection officer (DPO). The DPO will be responsible for independently supervising how data is stored, used and shared and for advising their organisation on data protection issues, reflecting the role that DPOs already play in the EU institutions.

Much work remains to be done before May 2018. The EDPS will continue to support the EU institutions and national data protection authorities (DPAs) to ensure that the new rules are successfully implemented.

The full text of the GDPR can be found in the *Official Journal*. To compare the negotiating texts of each of the institutions alongside the final text, you can download the *EDPS app*.

IT POLICY

Attempting to understand artificial intelligence

Artificial intelligence is a topic of increasing interest in the IT policy ccommunity. It was a point of discussion at the annual *International Conference of Data Protection and Privacy Commissioners*, which took place from 17-20 October 2016, and is the subject of an EDPS *background paper*. However, though the new technologies associated with artificial intelligence undoubtedly offer exciting possibilities for the future, they also represent a significant challenge for data protection.

Artificial intelligence is *defined as the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation*. Much research on the topic has so far focused on machine learning, which involves the construction of algorithms that can learn from and make predictions using data. Some well-known examples include *IBM Watson* and *Apple Siri*.

However, the way in which these machines *learn*, through applying algorithms to data, means that, in most cases, the models or *knowledge* produced by them cannot be understood by humans. This has serious implications for data protection. If we are unable to access information about how our data is processed by these machines and, more importantly, how decisions which concern us are taken by them, it is impossible for us to meaningfully consent to the processing of our data. Getting the right information can be further complicated by organisations claiming secrecy over how data is processed, on the grounds of trade secrets.

As the technology develops, we need to make sure that we are prepared for the changes it will bring. Data protection authorities (DPAs) will soon find themselves faced with cases in which machine learning has been used for taking or supporting a decision. Without any comprehensible model to analyse, deciding whether an individual's data protection rights have been breached or not will require analysis of the machine learning process itself. DPAs may soon need to decide whether they should develop their own pool of artificial intelligence experts and resources to be able to re-create and analyse the artificial intelligence models used by the organisations under their supervision.

EDPS Background Paper

Keeping internet traffic management under control

Internet Service Providers (ISPs) enable us to access the online world. This might be through a desktop, laptop, smart TV, connected utilities monitoring and controlling devices in the home or even a smart health device. As all our online activities pass through an ISP, unauthorised access to it could disclose a complete picture of our identity and habits. It is therefore essential that their use is effectively regulated.

One of the operations performed by ISPs is the management of internet traffic to avoid congestion, to ensure network security and, in certain circumstances, to ensure appropriate bandwidth for some specialised services, such as video streaming.

On 30 August 2016 the Body of European Regulators for Electronic Communications (BEREC) published its *Guidelines to National Regulatory Authorities (NRAs) on the implementation of the new net neutrality*. These Guidelines clarify and elaborate on the provisions of *Regulation (EU) 2015/2120*, which, among other things, includes rules to ensure that internet traffic management cannot be used as an opportunity to monitor personal data through ISPs.

The EDPS has followed net neutrality and traffic management issues since the Commission issued its *initial legislative proposal* in 2011. The Guidelines represent a step towards better protection for our personal data and privacy and effectively incorporate our views on the subject. Specifically, they state that, where the processing of personal data by ISPs occurs, it must be both necessary and proportional to achieving the specific objectives of traffic monitoring outlined in the Regulation. NRAs should ensure that a clear and comprehensive explanation of all traffic management measures and how ISPs ensure the privacy of their users when managing traffic is both published and included in the ISP contract. The Guidelines explicitly allocate the task of assessing compliance with applicable data protection law to the competent data protection authorities (DPAs).

ISRM and DPIAs: what they are and how they differ

In our *July Newsletter*, we presented our *Guidance on Information Security Risk Management* (ISRM). ISRM is a general requirement for data protection and will remain so under the new General Data Protection Regulation (GDPR). However, in addition to ISRM, the GDPR introduces a new obligation, requiring all organisations (*data controllers*) to perform data protection impact assessments (DPIAs) under certain conditions.

While the ultimate aim of both ISRM and DPIAs is to ensure that the fundamental rights of individuals are respected when their personal data is processed, DPIAs are much broader in scope. It is important to understand the difference between the two in order to use them effectively.

The starting point for both is a risk assessment. However, while ISRM only considers security risks, a DPIA addresses all data protection obligations. Therefore, while information security may be among the risks taken into account in a DPIA, an information security risk assessment on its own would not be sufficient to achieve the goals of the DPIA.

DPIAs are used to determine at an early stage if the intended use of personal data might violate an individual's right to data protection, so that planned data processing operations may be adapted accordingly to ensure compliance. They are particularly useful in demonstrating compliance with data protection rules, and therefore upholding the principle of *accountability*.

The EDPS supported the inclusion of both ISRM and DPIAs in the GDPR. It is now essential to ensure that *data controllers* understand the difference between these two measures and what they involve to ensure that these important and complementary obligations are effectively put into practice.

EDPS Guidance on ISRM

Unblocking the technology behind bitcoin

In the wake of a banking or currency crisis people often seek alternative ways of protecting their money. In the past this might have involved investing in gold or other valuables, but, more recently, digital innovations, such as *virtual currencies*, have become an increasingly popular option. The privacy implications of a switch to virtual currencies, however, are yet to be determined.

The most popular virtual currency, *bitcoin*, uses *blockchain technology*, a kind of digital transaction ledger secured by cryptography. This blockchain is public and cannot be altered, meaning that every bitcoin transaction, including any personal data associated with the transaction, is accessible to all. As the processing of data in the blockchain is shared among all bitcoin users, it is difficult to determine who is responsible for processing what data and how the basic principles of data protection, such as lawfulness, purpose limitation or data subject rights should be implemented.

It is essential that data protection experts begin to examine the concepts behind blockchain technology and how it is implemented in order to better understand how data protection principles can be applied to it. An integral part of this process should be the development of a privacy-friendly blockchain technology, based on the principles of *privacy by design*.

EVENTS

Confronting the challenges of Big Data

On 29 September 2016, the EDPS, in collaboration with European consumer organisation BEUC, hosted a *joint conference* on *Big Data: individual rights and smart enforcement*, in Brussels. The conference included panels on online platforms, smart technologies and the Digital Single Market. Speakers included EU Commissioner for Competition Margrethe Vestager, Federal Trade Commissoner Terrell McSweeny, BEUC Director General Monique Goyens, European Data Protection Supervisor Giovanni Buttarelli and European Commission Director General for Communication, Roberto Viola, and Director General for Justice, Tiina Astola.

Big Data and the Internet of Things pose policy, regulatory and enforcement challenges. Confronting these challenges requires a holistic approach to ensure that the rights and interests of individuals are safeguarded in the coming decades.

This high level conference brought together leading regulators and experts in the competition, data protection and consumer protection spheres to discuss key areas of economic and societal change, to promote closer dialogue and cooperation among regulatory and enforcement bodies and to explore how to better respond to the challenges our society is facing.

More information about EDPS work on big data can be found on the *EDPS website.*

For a more detailed report on the event, visit the *EDPS blog*.

IPEN: promoting privacy by design

On 9 September 2016, Goethe University Frankfurt hosted the most recent *IPEN workshop,* which was supported by the projects *CREDENTIAL* and *PRISMACLOUD*.

Following the *ENISA Annual Privacy Forum* which took place at the same location on 7-8 September 2016, a major topic of discussion was the practical impact of the GDPR.

Under the new rules, organisations (*data controllers*) are required to apply the principle of *data protection by design and by default* when processing personal data. While this principle is only directly applicable to the activities of data controllers and *processors*, manufacturers have also been strongly encouraged to apply data protection by design in developing their products and tools. Our discussions at the workshop produced several ideas on how best to promote this approach. These included:

- translating the requirements of the GDPR into design requirements and educating developers on these;
- starting to adopt privacy by design and by default in public administration and thus in public procurement;
- finding competitive advantage in developing privacy friendly technology and products;
- supporting users and giving them the tools to assess how privacy friendly a product is;
- enforcement of the principle by DPAs.

Participants also discussed technical and legal developments related to *privacy engineering*. This included a presentation on the current efforts to define *privacy engineering as a field*. Several technology development projects were presented and the privacy experts present provided valuable feedback and ideas for improvement.

The workshop confirmed that the direct exchange between (legal) privacy experts and technology developers is useful and necessary. It is vital that this exchange continues.

Digital Festival 2016

Digital Festival 2016 took place at The Egg in Brussels on 21 June 2016. Branded as a *festival of ideas*, the event provided an opportunity to challenge and better understand the impact and potential of digital technologies.

As part of the festival, the EDPS organised a workshop entitled *Data Protection by Design: Privacy as an engineering principle*. It addressed the different approaches to privacy engineering, the current challenges faced and initiatives, such as the *Internet Privacy Engineering Network* (IPEN), which aim to overcome these challenges. This is particularly important area of discussion, given that the new EU data protection rules, to be applied by May 2018, make the implementation of *data protection by design* and by default a legal obligation for all organisations involved in the processing of personal data.

The workshop was moderated by EDPS IT Policy leader Achim Klabunde. Other speakers included data analyst and entrepreneur Aurelie Pols, digital activist Estelle Masse from AccessNow, Researcher Jetzabel Serna from Goethe-University Frankfurt and Aristotelis Tzafalias from the European Commission.

SPEECHES AND PUBLICATIONS

- "Adequacy, Localisation and Cultural Determinism", keynote speech (*PDF*) given by Giovanni Buttarelli at the 38th International Privacy Conference, Marrakech, Morocco (19 October 2016)
- "The impact of the General Data Protection Regulation on collaborative science in Europe and the European Cloud Initiative", speech (*PDF* and *video*) given by Giovanni Buttarelli at the ISC Intelligence in Science Seminar, Brussels (18 October 2016)
- Keynote speech (*PDF* and *video*) given by Giovanni Buttarelli at the Belgian Senate Conference - Issues of citizens' privacy and data protection in relation to new technologies, Brussels (17 October 2016)
- "The accountability principle in the new GDPR", speech (*PDF*) given by Giovanni Buttarelli at the European Court of Justice, Luxembourg (30 September 2016)
- Closing speech (*PDF*) given by Giovanni Buttarelli at the EDPS-BEUC joint conference, Brussels (29 September 2016)
- "Big Data individual rights and enforcement", speech (*PDF*) given by Giovanni Buttarelli at the EDPS-BEUC joint conference, Brussels (29 September 2016)
- "Data Protection rules in relation to financial services and digital economy", speech (*PDF*) given by Giovanni Buttarelli at BBA's Data Protection & Privacy conference, London, United Kingdom (15 September 2016)
- "Global Personal Data Protection Policy Trend", keynote speech (*PDF*) given by Giovanni Buttarelli at the Korea Internet and Security Agency (KISA), Seoul, South Korea (18 July 2016)
- Keynote speech (*PDF*) given by Giovanni Buttarelli at the BEUC Digiforum 2016: Consumers shaping the digital economy, Brussels (20 June 2016)
- "Key Challenges for Privacy in the Digital Age", speech (*PDF*) by Giovanni Buttarelli to Europol/EIPA conference on Privacy in the Digital Age of Encryption and Anonymity Online, The Hague (19 May 2016)
- "European Union as a promoter of a real revolution", article (*PDF*) by Giovanni Buttarelli in Il Sole 24 Ore newspaper (9 May 2016)
- "Counterterrorism and Data Privacy: A European Perspective", speech (*PDF*) given by Giovanni Buttarelli to the symposium on Governing Intelligence: Transnational Approaches to Oversight and Security, hosted by the Center on Law and Security and the Woodrow Wilson International Center for Scholars, New York (21 April 2016)
- "Ethics at the Root of Privacy and as the Future of Data Protection", address (*PDF*) given by Giovanni Buttarelli at event hosted by Berkman Center for Internet and Society at Harvard University and the MIT Internet Policy Initiative and the MIT Media Lab (19 April 2016)

DATA PROTECTION OFFICERS

Recent Appointments:

- Mr. Pierre Faller, European Foundation for the Improvement of Living and Working Conditions (Eurofound)
- Mr. Christos Georgiadis (DPO) and Mr. Ramunas Lunskus (Alternate DPO), European Institute for Gender Equality (EIGE)
- Ms. Radostina Nedeva Maegerlein, European Maritime Safety Agency (EMSA)
- Ms. Ena Ostroski (Acting DPO), Body of European Regulators for Electronic Communications (BEREC)
- Ms. Elke Riviere (DPO) and Mr. Anthony Bisch (Deputy DPO), Executive Agency for Small and Medium-sized Enterprises (EASME)
- Ms. Triinu Volmer (DPO) and Ms. Matxalen Sanchez Exposito (Deputy DPO), European GNSS Supervisory Authority (GSA)
- Ms. Marina Zuback, Agency for the Cooperation of Energy Regulators (ACER)

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-16-002-EN-N ISBN 978-92-95073-01-2 doi:10.2804/985165