EDPL EUROPEAN DATA PROTECTION LAW REVIEW

Your biweekly news on EU data protection
For more in-depth analysis go to lexxion.eu/edpl

Data Protection Insider

Issue 12, 28 November 2019

- Wojciech Wiewiórowski Elected as European Data Protection Supervisor -

Following the voting procedure outlined in Regulation 2018/1725 – the Data Protection Regulation for EU Institutions' – Wojciech Wiewiórowski has been elected as the new European Data Protection Supervisor. He was chosen over two other candidates: Yann Padova (France) and Endre Szabó (Hungary). Mr. Wiewiórowski has already been at the EDPS for several years – initially as Assistant EDPS and, following the death of Giovanni Buttarelli earlier this year, as acting EDPS. He will now serve a five-year term as the EDPS. We would like to congratulate Mr. Wiewiórowski – also a Board Member at EDPL. We look forward to his term and to seeing how he develops the office.

Learn more

- EDPB Adopts Four Documents -

On November 12th and 13th the EDPB met in plenary session. As a result of the session, the EDPB adopted the following six documents:

- Report on the Third Annual Joint Review of the EU-US Privacy Shield
- Guidelines on the Territorial Scope of the GDPR (version following public consultation)
- Guidelines on Data Protection by Design and by Default
- Article 64 Opinion on ExxonMobil BCRs
- Response letter to LIBE on EU Information Systems
- Contribution to the consultation on a draft second additional protocol to the Budapest Convention on Cybercrime

Each of the documents is now available for download from the EDPB's website.

Learn more

- EDPB Documents: A Focus on the Guidelines on Territorial Scope -

One of the documents adopted in the EDPB's plenary session was a set of Guidelines on the Territorial Scope of the GDPR. The Guidelines provide extensive technical clarifications of the concepts relating to territorial scope in the GDPR. Clarifications are offered, for example, in relation to: the applicability of the 'establishment criterion' in Article 3(1) GDPR; the applicability of the 'targeting criterion' in Article 3(2) GDPR; and the requirement to designate, and the role of, a representative for controllers or processors not established in the EU in Article 27 GDPR. In terms of substance, the Guidelines employ an overtly broad interpretation of the GDPR's concepts of territorial scope – hardly a surprise given the language of the GDPR concerning territorial scope – but contain few surprises. On the one hand, the Guidelines are most welcome in clarifying and concretizing an area of confusion in the GDPR. On the other hand, the Guidelines do not provide much in the way of answers to the more interesting questions concerning the GDPR's territorial scope. For example, the Guidelines do not provide any answers to questions concerning the basic legitimacy of the extra-territorial applicability of EU law or to questions concerning the practicalities of the extra-territorial enforcement of EU law. To blame the Guidelines for not providing such answers would, however, be largely unfair. Answers to these questions will eventually require international political and juridical collaboration. The structures through which this collaboration might emerge, however, have not yet crystallized.

Learn more

- E-Privacy: Presidency Draft Rejected by Council -

On 22 November 2019, the EU Member States, assembled in the Council of the European Union, rejected the Finnish Council presidency‘s proposal for an e-Privacy Regulation. Amongst other objectives, the Finnish Presidency’s proposal aimed to bring online communications providers such as Skype and Whatsapp under the same confidentiality rules as traditional telecommunication providers and to increase protection for citizens offered by these rules. A cursory look at the publicly available information is not revelatory as to why Member State governments rejected the proposal. According to Euractiv, however, reasons included disagreements over the regulation of tracking cookies, consent and the detection of child pornography. The next steps for the e-Privacy Regulation are now unclear. What is certain is that the legislation cannot be adopted without the adoption of a common position in the Council. It remains to be seen whether the next Council Presidency – the Croatian Presidency – will resume the negotiations. The lack of progress on the proposed e-Privacy Regulation after leaves the legislative framework around the confidentiality of online communications with obvious substantive flaws – for example the lack of applicability to over-the-top content. In addition, the protection offered by the existing e-Privacy Directive is no longer completely aligned with the protection provided by the GDPR. Given the obvious need for an update of the e-Privacy framework, the fact that Member States cannot reach an agreement is perplexing. Do the reasons relate solely to technical discussions in the Council, or are there other influences at play?

Learn more

- UN Human Rights Expert Concerned about Digital Welfare Dystopia -

In a newly released report, Philip Alston, UN Special Rapporteur on extreme poverty and human rights, has warned that the digital revolution might be leading us into a ‘digital welfare state’. He is concerned that this ‘digital welfare state’ aims at reducing welfare spending, increasing government surveillance and advancing private corporate interests. He notes that many analyses have been made about the risks e-Government applications, and especially Artificial Intelligence, pose for human rights. However, according to him, none of these analyses ‘has adequately captured the full array of threats represented by the emergence of the digital welfare state’. This is an astute observation. It is indeed the case that e-Government technologies and AI have received a lot of attention, especially in the privacy and data protection discourse. Perhaps part of the reason for the lack of holistic consideration of issues is the focus on privacy and data protection as the fundamental rights loci for identifying problems associated with disruptive technologies and the state. Given that the use of digital technologies is having such evident and profound impact on basic social facts and institutions, surely these impacts need to be considered in light of a broad panoply of rights – rather than always in terms of privacy and data protection? Conversely, if we insist on considering all aspects of the digital society through the lens of privacy and data protection, how long before it becomes logical to consider the rights to privacy and data protection as umbrella terms for collections of cogent sub-rights?

Learn more

- Bulgarian Data Protection Law: Between Data Protection and Freedom of Expression -

On 15 November 2019, the Bulgarian Constitutional Court declared Article 25(z)(3) of the Bulgarian Data Protection Act – which implements Article 85 GDPR on the balance of data protection and freedom of expression – unconstitutional. The contested provision enshrined 10 criteria for balancing data protection with freedom of expression. The judges found that these criteria were too vague and opened the door to arbitrary enforcement by the Bulgarian Data Protection Commission. The judges also found that use of the criteria could have a chilling effect on free media – for example by stifling pluralistic debate around the activities and policies of the government. Four of the twelve judges sitting on the case issued a joint dissenting opinion. Without going into the details of the judgment and the dissenting opinion, it is not surprising to see challenges to national implementing provisions of Article 85 GDPR. The balance between the two fundamental rights at stake is a delicate one – perhaps the reason the CJEU seems so reluctant to weigh in on the correct balance, as in Google Spain. Indeed, it might legitimately be questioned as to whether a hard regulation of the balance between these rights is possible or desirable. Another interesting aspect of the judgment is the concern that the Data Protection Commission had disproportionate power in deciding on the fair balance on a case-by-case basis. This concern is, to some extent, understandable. If the power to decide on such balances in relation to data processing should not be left with DPAs, however, then with whom should it rightfully be left?

Learn more

- Apps more Data Protection Friendly after the GDPR -

Research has just been published concerning the degree to which apps seek to process personal data following the applicability of the GDPR. Researchers from Karlstad University and Goethe University engaged in a survey of the data collection practices of 50 popular apps both prior to, and subsequent to, the applicability of the GDPR. A comparison of data collected in the two time periods showed that apps, on average, collected and processed less user data following the applicability of the GDPR. The researchers point out, however, that apps still tend to collect more user data than is necessary for the fulfilment of the services offered. The results of the research are interesting for several reasons. Two reasons stand out. First, the research offers empirical evidence as to how the GDPR is impacting the processes and practices of the information ecosystem – or at least a significant sector of the information ecosystem. Such empirics are particularly valuable in privacy and data protection discussions, which tend to remain highly doctrinal. Second, the research appears to verify that the GDPR is influencing data collection and processing practices. Claims as to the impact of the GDPR on data processing intuitively seem correct and are, accordingly, often put forward – by a variety of actors supporting a variety of normative positions. Yet hard evidence providing depth and texture to such claims has been comparatively lacking. It remains to be seen whether the trend toward more data protection friendly apps will continue. It also remains to be seen whether this trend indicates a change in the culture and mentality of app developers, or whether the change simply reflects the acceptance of an unwelcome legal imposition.

Learn more

Meet the Editors:


© FIZ Karlsruhe

Dara Hallinan, Editor: Legal academic working at FIZ Karlsruhe. His specific focus is on the interaction between law, new technologies – particularly ICT and biotech – and society. He studied law in the UK and Germany, completed a Master's in Human Rights and Democracy in Italy and Estonia and wrote his PhD at the Vrije Universiteit Brussel on the better regulation of genetic privacy in biobanks and genomic research through data protection law. He is also programme director for the annual Computers, Privacy and Data Protection conference.


© FIZ Karlsruhe

Diana Dimitrova, Sub-editor: Researcher at FIZ Karlsruhe and PhD candidate at Vrije Universiteit Brussel. Focus on privacy and data protection, especially on rights of data subjects in the Area of Freedom, Security and Justice. Previously, legal researcher at KU Leuven and trainee at EDPS. Holds LL.M. in European Law from Leiden University.

Learn more about EDPL

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu
