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 7, 19 September 2019

- The New Commission: Who Is in Charge of Data Protection? -

Last Tuesday, President-Elect Ursula von der Leyen presented the new EU Commissioner-designates and their portfolios. The new Commission and the individual Commissioners still need to be confirmed by the European Parliament. Provided no changes are introduced, data protection topics will now fall under 4 different portfolios. First, the new Executive Vice-President for a "Europe fit for the Digital Age" (Margrethe Vestager) will coordinate the different policy aspects concerning digitalization and thus the work of the other relevant Commissioners. Emphasis has been placed on industry, SMEs, Artificial Intelligence, digital taxation and the Digital Services Act. Second, the Commissioner for Justice (Didier Reynders) will be responsible for the GDPR and the "human and ethical implications of artificial intelligence." Third, the Internal Market Commissioner (Sylvie Goulard) will be responsible for enhancing Europe's technological sovereignty, AI, the Digital Services Act and single market for cybersecurity. Fourth, The Vice-President for Values and Transparency (Vera Jourova) will oversee the application of the EU Charter of Fundamental Rights. On the one hand, it is positive that that an Executive Vice-President will coordinate all aspects of digitalization. On the other hand, however, it remains to be seen how smoothly this coordination will run and whether the new Commission structure can achieve harmony between the different aspects of digitalization it outlines.

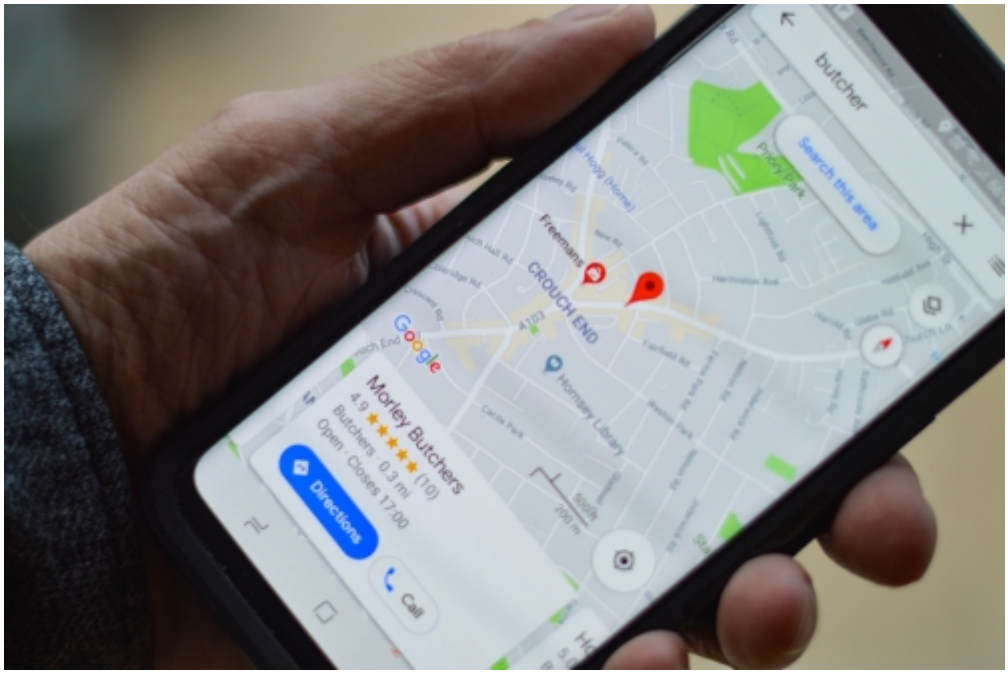
Learn more

- Prisoner Surveillance in Russia Infringes Privacy -

In the Izmestyev v. Russia case (application no. 74141/10), the ECtHR held that the video surveillance to which the applicant was subject in his prison cell violated Article 8 ECHR. The grounds for the infringement lie, according to the Court, in the fact that applicable Russian law was not formulated with sufficient clarity to determine whether the use of video surveillance in prison was restricted to what is "necessary in a democratic society." The Court held that the lack of clarity breached the foreseeability and accessibility of the law requirement, as it did not prescribe and restrict the use of video surveillance in any way. The Court rejected the arguments of Russian domestic courts that prisoner surveillance should be expected by detained individuals and no special legitimating measures should be necessary. The judgment is notable for two reasons. First, the Court, once again, has focused its examination of surveillance issues on the quality-of-the-law

criterion rather than on the question of the necessity and proportionality of the surveillance as such. Second, the case is another in a string of cases dealing with surveillance in Russia. ECtHR decisions on Russia are passed in a politically charged atmosphere. It would not be surprising if this atmosphere impacted the Court's reasoning – the idea of constitutional courts as political entities is not new. If this is the case, this begs the question as to how such cases should be dealt with as part of the Convention's surveillance jurisprudence. From a legal positivistic perspective, these cases constitute jurisprudence like any other. Yet, if politics plays a role in the formulation of the judgment, should this not be considered in weighting the content of such judgments against other comparable jurisprudence? It would be fascinating to see more work on this issue.

Learn more

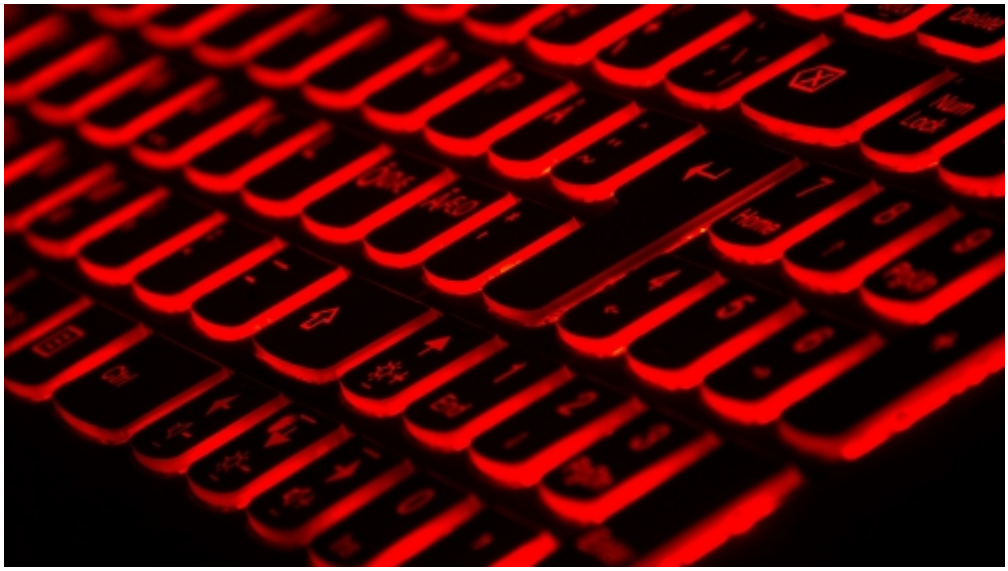


- Location Data not Mature Enough for Police Investigations -

The Danish justice system has discovered weaknesses in the use of geolocation data for investigating crimes. In a review, the justice system highlighted two key problems. First, the software that converts raw data from phone masts into geolocation evidence omits relevant data – e.g. of some of the calls made to and from a phone number. Second, the technology used can link phones to the wrong masts. As a result, the final analysis cannot provide law enforcement with geolocation data of adequate precision to ascertain the location of the person under investigation. Law enforcement authorities acknowledge the insufficient quality of the data could lead to miscarriages of justice. Telecom providers maintain it is their job to provide telecommunication services and not evidence in criminal cases and cannot bear responsibility for the usefulness of telecom data for law enforcement. As a result of the review, 32 prisoners have been released. The Danish review has broader significance for several reasons. First, this is the first time that a national justice system has questioned the

quality of geolocation information. Second, the review adds another dimension to the ongoing discussion around bulk telecommunications surveillance. The accuracy of the raw and derived surveillance data had hitherto been relatively underdiscussed. Third, the story provides a prime example of how data deemed of sufficient quality for one purpose may be of inadequate quality for a different purpose. The review may impact other policies – e.g. on the interoperability of different databases, such as in the Area of Freedom, Security and Justice.

Learn more



- Brexit, and Data Protection as a Tool of Politics -

A legal opinion has been put forward suggesting a UK Conservative Party website is illegitimately collecting user data to use in political advertising in support of Brexit. Specifically, the opinion asserts the website is not offering users adequate information on the use of their personal data for targeted political advertising. The opinion is interesting for two reasons. First, the substance of the opinion is fascinating – elaborating a position on what

should, or should not, count as adequate transparency and consent in relation to targeted political advertising. Second, the opinion reflects a deeper development in the social function and use of data protection law: data protection law as a tool of politics. The opinion was requested by the Good Law Project, an initiative which aims to use the law to deliver a more progressive society and which is explicitly anti-Brexit. Data protection law, in this case, has been used in a targeted fashion to undermine a Brexit supporting website – a political opponent. There is a clear, burning, and very public, conflict between the need for data protection – and the rights it protects – and the hunger of modern election campaigns for personal data. In this environment, data protection becomes capable of fulfilling several roles in furthering political agenda – discrediting the morality of an opponent through highlighting illegitimate data processing practises etc. As personal data become ever more important in politics, look for this function of data protection to grow in parallel.

Learn more

- DPA Push for Children's Privacy -

In the past two weeks, the Irish and the French DPAs have been active with respect to children's privacy. The Irish DPA, in an interview with Bloomberg Law, asserted they were actively 'scoping' children's privacy enforcement actions under the GDPR and suggested they saw the need for significant changes in practise. The French DPA has issued guidance for parents concerning the privacy implications, and how to deal with them, of providing smartwatches to children. The theme of children's privacy has received comparatively little attention from DPAs and lawmakers to date. This lack of attention is regrettable considering both the vulnerable position of children in relation to data controllers as well as the degree to which children are exposed to, and immersed in, the information society. The fact that two DPAs, in such a short space of time, have felt it worthwhile to focus on children's privacy is a sign the theme may be gaining momentum.

Interestingly, these moves are concurrent with Google paying $170 million to settle US Federal Trade Commission claims the company infringed US law on children's privacy.

Learn more

- UK DPA Issues Guidance on No-Deal Brexit -

The UK DPA – the ICO – has issued guidance for small and medium sized companies on the possibility of a no-deal Brexit. The guidance predominantly deals with how companies can engage in data transfers between the UK and Europe if no-deal comes to pass. The guidance is interesting for two reasons. First, the guidance highlights the fact that the ICO are now, publicly, beginning to seriously plan for a no-deal Brexit – perhaps unsurprising given the current Brexit deadline at the end of October and the apparent lack of progress in talks. Second, the guidance highlights that, in the event of a no-deal Brexit, the UK will be regarded as a third country and that, under the GDPR, transfers will need to happen based on standard contractual clauses or some other legitimate basis. This raises the further question as to how the situation will subsequently develop. Even in a no-deal scenario, the UK will retain the GDPR as the substantial template for national law and will remain party to all relevant international data protection instruments. The UK would, logically – presuming no seismic shifts in politics – be substantially suitable for immediate adequacy status. Yet, an adequacy status can only follow an adequacy procedure and the current adequacy procedure has significant limitations. This is true in terms of capacity of the procedure – only very few countries can go through the procedure at one time and each procedure can take several years. This is also true in terms of the substance of the procedure – the procedure has shown itself to be politicized in the past. This raises the question as to when, and the degree to which, substantive compatibility between UK and EU data protection regimes will suffice for adequacy.

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

Recommend this newsletter. If you were forwarded this email, subscribe here https://www.lexxion.eu/en/newsletter/


Image

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu