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 16, 6 February 2020

- ECtHR Rules on Telecommunications Subscriber Registration -

On 30th January, the ECtHR ruled on the *Breyer* case. The facts of the case were as follows: two German nationals bought pre-paid SIM cards. In the course of buying these SIM cards, they were required to provide certain personal information – including, for example, names, addresses, telephone numbers, dates of birth etc.. This information, in line with Article 111 of the German Telecommunications Act, was required to be stored and, in line with Articles 112 and 113 of the same act, could be accessed and used by a number of German authorities – mostly for the prevention and detection of crime. The applicants challenged Articles 111, 112 and 113 of the Telecommunications Act on the basis these required a disproportionate collection and processing of their personal data and constituted an infringement of Article 8 – right to respect for private and family life – and Article 10 – freedom of expression – rights under the ECHR. The Court found no violation of Article 8 and did not consider Article 10. Whilst many in the data protection community may have expected a judgment with high significance for EU data retention discussions, this is not what has been delivered. The Court was cautious to highlight the substantial difference between the issues at hand in the case – the collection of subscriber data – and those in EU data retention discussions – the retention of communications metadata. Even in the judgment delivered, the Court left significant issues open. Two stand out. First, the Court made several statements as to the existence and function of safeguards concerning official access to stored data. The Court failed, however, to provide extensive explanation of the reasoning behind some of these statements – for example: 'the obligation to submit a written request for information was likely to encourage the authority to obtain the information only where it was sufficiently needed'. Second, the Court recognised that legal obligations to retain subscriber personal data to combat crime represented a reasonable response in relation to 'changes in communication behaviour and in the means of telecommunications'. The Court failed, however, to elaborate why the lack of empirical evidence that such retention led to a reduction in crime should not be considered in evaluating the reasonableness of the measure.

Learn more

- EDPB Adopts Seven Documents -

On 28th and 29th January, the EDPB had its 17th plenary session. As a result of the session, the EDPB adopted the following seven documents:

- Opinions on the Accreditation Requirements for Codes of Conduct Monitoring Bodies submitted to the Board by the Belgian, Spanish and French supervisory authorities (SAs).
- Draft Guidelines on Connected Vehicles.
- Final version of the Guidelines on the processing of Personal Data through Video Devices following public consultation.
- Opinions on the draft accreditation requirements for Certification Bodies submitted to the Board by the UK and Luxembourg SAs.
- Opinion on the draft decision regarding the Fujikura Automotive Europe Group's Controller Binding Corporate Rules (BCRs), submitted to the Board by the Spanish Supervisory Authority.
- A letter in response to MEP Sophie in't Veld's request concerning the use of unfair algorithms.
- Letter to the Council of Europe on the Cybercrime Convention.

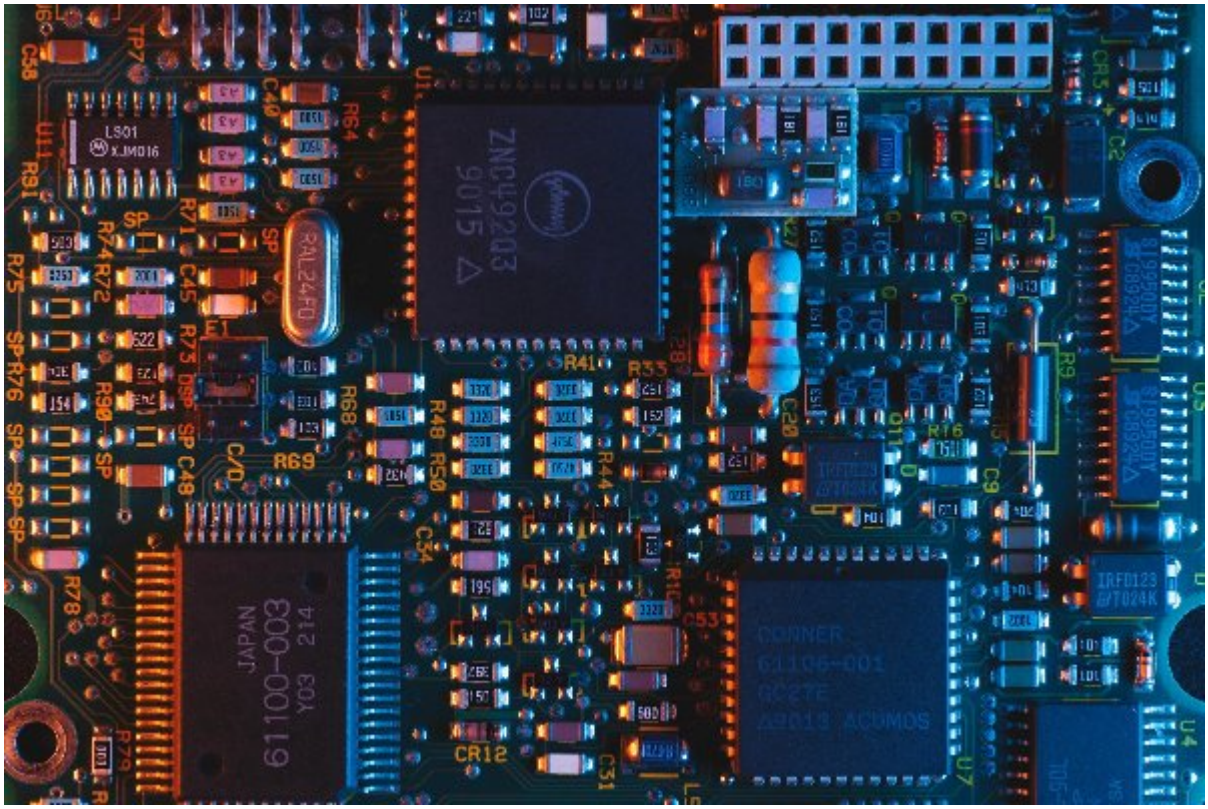
The documents are not yet available on the EDPB website. The documents will be made available over the course of the coming days and weeks following the necessary legal, linguistic and formatting checks.

Learn more

- AG Opinion on Access to Telecommunications Data -

On 21st January Advocate General Pitruzzella delivered his Opinion in response to three preliminary ruling questions by the Estonian Supreme Court concerning access by law enforcement authorities to telecommunication data under Article 15 (1) Directive 2002/58. In response to these three questions, AG Pitruzella came to two significant conclusions. First, the AG argued that the categories of data collected, the temporal period in respect to which access to data are sought and the seriousness of the crime in question should be taken into account in evaluating the proportionality of an interference with fundamental rights. Second, the AG argued that the requirement for independent review of the application for access to telecommunications data is not fulfilled where the review is carried out by a public prosecutor's office which then represents the public prosecution in subsequent judicial proceedings. The Opinion is further interesting from two perspectives. First: from the perspective of the questions the Opinion did not (wish to) answer. In the case, the CJEU was asked – by the European Commission – to rule on the compatibility of data retention as such with the CFREU. The AG, however, preferred not to directly answer this question. Instead, he merely observed: i) pursuant to the CJEU's existing case-law, general and indiscriminate retention is not compatible with the CFREU, and ii) that the Opinion of AG Campos Sánchez-Bordona from 15th January – which referred to the concept of "limited data retention" – also did not exclude general retention in exceptional circumstances. Unfortunately, neither existing case law, nor the Opinion of AG Campos Sánchez-Bordona, provide clarity or finality in relation to the question of the legitimacy of data retention as such. Second, from the perspective of the argumentation employed in relation to the questions the Opinion did answer. The referring Court sought guidance as to whether access to telecommunication data should be restricted to serious crimes only. The AG concluded that Article 15(1) Directive 2002/58 does not preclude access to this data in relation to serious crimes only. This seems contrary to CJEU's prior conclusion in *Tele2*. In addition, AG Pitruzella did not provide detailed argumentation as to why access should be granted also in the framework non-serious crimes, beyond simply stating that serious crime is defined differently in different Member States and that sometimes the seriousness of the crime cannot be defined at the beginning of an investigation. The AG failed to observe, however, that there are cases where EU law already provides a clear list of offences which are considered serious – e.g. the case of retention of PNR data.

Learn more



- The European Commission Publishes Working Programme 2020 -

On 29th January the European Commission published its Working Programme 2020. Annex I provides an informative overview of the upcoming 43 legislative and non-legislative initiatives. Of these, the following nine are digital policies and will likely have an impact on data protection:

- A Strategy for Europe - Fit for the Digital Age (non-legislative, Q1 2020);
- White Paper on Artificial Intelligence (non-legislative, Q1 2020);
- European Strategy for Data (non-legislative, Q1 2020) concerning non-personal data;
- Follow-up to the White Paper on Artificial Intelligence, including on safety, liability, fundamental rights and data (**legislative**, incl. impact assessment, Article 114 TFEU, Q4 2020);
- Digital Services Act (**legislative**, incl. impact assessment, Article 114 TFEU, Q4 2020);
- Review of the Directive on security of network and information systems (NIS Directive) (**legislative**, incl. impact assessment, Article 114 TFEU, Q4 2020);
- New Strategy for the Implementation of the Charter of Fundamental Rights (non-legislative, Q4 2020);
- Report on the application of the General Data Protection Regulation (GDPR) (non-legislative, Q2 2020);
- Alignment of relevant Union law enforcement rules with regard to data protection (non-legislative, Q2 2020)

Most innovative is the Commission's proposal for a legislative instrument on Artificial Intelligence, including on fundamental rights and data – presumably focused on data protection and privacy. The other topics are not as novel and refer to pre-existing EU initiatives. Amongst these topics, it will be interesting to see how the Commission envisages implementing the much-needed alignment of law enforcement rules with respect to data protection. This intended alignment surely implies an amendment to all existing relevant instruments. This is, of course welcome, given it is almost 4 years since Directive 2016/680 entered into force. This raises the question as to why these instruments have not been amended so far, given it is almost 4 years since Directive 2016/680 entered into force?

Learn more

- ICO Release Statement on Brexit -

On the 29th of January, shortly prior to the UK leaving the EU, the ICO issued a statement about Brexit and EU-UK personal data flows. The focus of the statement is on the transition period, which will last until the end of December 2020. In this regard, the ICO state: 'it will be **business as usual** for data protection. The GDPR will continue to apply. Businesses and organisations that process personal data should continue to follow our existing guidance for advice on their data protection obligations.' The ICO do recognise later in the statement, however, that the situation regarding data protection and EU-UK data flows following the transition period remains unclear. The statement is certainly welcome for businesses and organisations wondering about the significance of leaving the EU for EU-UK data flows. Moving forward, it will be fascinating to see what the future holds for UK-EU data flows. Early signs, however, indicate the road to a final stable framework may be rough and that the final framework may be less than ideal. In this regard, three factors, in particular, are noteworthy. First, the initial positions taken in EU-UK transition negotiations are adversarial. It is true these initial positions may represent mere sabre-rattling and that, even if these positions are retained, smooth data flows may be insulated from other political discussions. There is, however, no guarantee this will be the case. Second, there are already indications that UK uses of personal data may be problematic for EU Member States and that such uses may stand as obstacles to simply granting the UK adequacy. Finally, adequacy procedures themselves are lengthy affairs and are subject to political manoeuvring. Even if the UK retains the GDPR – or a GDPR copy – and is, substantially, adequate in all other relevant respects, this is still no a guarantee that an adequacy decision will be granted fast, or even at all.

Learn more

- European Parliament Discuss Californian Adequacy -

Earlier this month, the European Parliament discussed the third annual review of the Privacy Shield agreement. The discussion was lengthy and several interesting, and differing, viewpoints, were presented. In the course of the discussion, however, one particularly interesting question emerged: should the Privacy Shield agreement ever be struck down, could California receive adequacy on its own? The discussion naturally emerged on the back of recognition of the strength, compared to federal protection, of the new Californian state data protection law, the CCPA. The discussion is interesting for several reasons. Two stand out. First, the discussion highlights the seldom-considered possibility for states, or territories, within countries, to apply for adequacy separately from the country itself – recall the discussions as to the adequacy of Quebec in 2014. Second, the discussion gives pause for serious reflection on the CCPA and other relevant Californian law, and their compatibility with European data protection laws. In the first instance, despite the fact the CCPA has been largely lauded in Europe for the strength of protection it offers, and even though it has even been referred to as a US GDPR, there remain significant differences between the CCPA and European data protection laws. Compare, for example, the scope of the CCPA as providing protection for consumers' personal data and the scope of the GDPR as providing protection for natural persons' personal data. In turn, even if the CCPA were a carbon copy of the GDPR, California is still a state in the US. Accordingly, California is still subject to federal laws. Some of these laws have been highlighted as problematic for EU data protection standards in the past and would need to be taken into account in any state adequacy process in the future.

Learn more

Meet the Editors:

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


© FIZ Karlsruhe

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/

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu
