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 14, 02 January 2020

- CJEU Rules on Surveillance Cameras -

On 11 December 2019, the CJEU ruled on a case concerning the proportionality of video surveillance. The case concerned the matter of whether the installation of video cameras in the entryway to an apartment complex aimed at preventing vandalism, constituted a disproportionate interference with surveilled individuals' rights. The CJEU's judgment revolved around the question: 'whether Article 6(1)(c) [Article 5(1)(c) GDPR] and Article 7(f) [Article 6(1)(f) GDPR] of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national provisions which authorise the installation of a system of video surveillance, such as the system at issue'. The CJEU decided, in line with previous case-law, that such national legislation was permissible providing it allowed for case-by-case proportionality calculations to be performed and the processing fulfilled the conditions of Article 7(f). In the most interesting part of the judgment, the CJEU elaborated on the three cumulative criteria for the applicability of Article 7(f): the existence of a legitimate interest; the necessity of a data processing measure in relation to achieving this interest; and the proportionality of the interference with subjects' rights caused by the data processing measure. The CJEU offered two particularly significant clarifications. First the CJEU clarified a measure can only be necessary when the aim of the measure could not be achieved either: by other means involving a lesser rights infringement; or by means involving less data processing. Second, the CJEU outlined a series of factors to be considered in a proportionality calculation. Amongst these, the CJEU specifically highlighted data subjects' expectations regarding processing as relevant.

Learn more

- AG Opinion in *Schrems II* -

On 19 December, AG Saugmandsgaard Øe delivered his Opinion in the second case of Schrems against Facebook. In the case, the referring Court raised questions as to the validity of SCCs. Specifically, the Court asked questions: concerning whether the lead data protection authority in Europe – the Irish DPA *in casu* – could suspend data flows based on the Commission's SCC; and concerning the validity of the Privacy Shield framework. In his opinion, the AG made several significant pronouncements. First, the AG first clarified that, whilst he found the text of the SCCs to be compatible with Articles 7, 8 and 47 CFREU, he also found the Irish DPA could still suspend data flows based on SCCs if irregularities were found in the data processing after transfer – i.e. in the USA. Second, the AG found that, because the data transfers in casu take place based on SCCs, the facts of the case did not necessitate the need to examine the validity or compatibility of Privacy Shield with EU data protection law. Despite this finding, the AG did go on to offer an extensive examination of the validity of Privacy Shield. In this examination, the AG raised serious doubts about the validity of Privacy Shield and the validity of the Commission's finding of an essentially equivalent level of data protection in the USA. Third, the AG clearly stated that the Commission adequacy finding in the framework of the Privacy Shield should not prejudice the Irish DPA's work in independently assessing the legality of transfers to the USA under SCCs. Interestingly, in his analysis of Privacy Shield, the AG referred both to the CFREU and the ECHR. Whilst the issue of bulk (communication) surveillance has been an issue before both the CJEU and the ECtHR, the Courts have approached the matter in different ways and appear to have come to different conclusions. It remains to be seen whether the CJEU will follow the AGs opinion.

Learn more

- New Data Protection Regime at Eurojust -

With the new Eurojust Regulation, Eurojust – previously one of the EU's bodies responsible for criminal justice cooperation – has been granted the status of an EU Agency and has been provided with a new legal basis. In data protection terms, the legal change implies two things. First, Eurojust now has a new data protection regime, which is now synchronised with the new EU data protection framework – including Regulation 2018/1725 applicable to the EU institutions, bodies and agencies. Second, The EDPS will take over the supervision of Eurojust's data processing practises, replacing the previously existing Joint Supervisory Body – composed of judges and/or data protection commissioners. With this change, the EDPS can now exercise its full range of supervisory powers over Eurojust – from starting its own inquiries, examining complaints and issuing orders, to filing cases against Eurojust with the CJEU. At the same time, the existing national data protection commissions will still retain certain supervisory powers – for example with regards to the supervision of data which national authorities forward to Eurojust. These developments are welcome as they continue the trend of breaking the data protection "wall" between ex-third pillar activities and other EU bodies/agencies. The developments also demonstrate the desire of law-makers to align the rules on data protection across sectors and institutions. It remains to be seen, however, whether these developments will, in fact, mitigate against fragmentation in data

protection rules. It also remains to be seen how smoothly the EPDS and national data protection commissions will cooperate.

Learn more

- EDPS Releases Guidelines on Proportionality -

The EDPS has released guidance on the concept of proportionality in relation to the adoption of measures involving the processing of personal data by EU institutions. The guidance builds on existing jurisprudence concerning the proportionality of the processing of personal data from the CJEU, the ECtHR, the Article 29 Working Party, the EDPS and the EDPB. The guidelines are to be welcomed for several reasons. Two are particularly noteworthy. First, the Guidelines provide clarification of the overlaps and differences between the related concepts of necessity and proportionality. Second, the Guidelines provide a structured and logical approach to the calculation of the proportionality of EU measures involving data processing. It remains to be seen whether, and how closely, the Guidelines are followed by EU institutions. It also remains to be seen whether the Guidelines – or parts of the Guidelines – are adopted or used in other contexts, for example by Member State DPAs. Looking to the future, the Guidelines provide a foundation on which guidance on proportionality in relation to private sector and Member State processing regulated by the GDPR might be built. Such guidance is sorely needed and would assist in better data controller understanding of numerous GDPR principles – the DPIA obligation in Article 35, for example.

Learn more

- Swedish Fine for Publishing Credit Information -

The Swedish Data Protection Authority has imposed a 35,000 Euro fine on the website Mrkoll.se. Mrkoll.se publishes personal information on all Swedes above 16 years of age. For that purpose, and in line with the Swedish constitutional right to freedom of expression, Mrkoll.se possesses a publishing certificate which applies to most of its activities and exempts them from the requirements of the GDPR. However, in this case, the website published two types of information for which this exemption did not apply. First, the website published information on payment defaults. These are legally defined in Sweden as credit information and their publishing must therefore comply with the Credit Information Act. This act contains explicit references to the relevance of provisions of the GDPR. Second. The website published information on criminal convictions, which, according to the Credit Information Act are regulated by the GDPR. This is not the first time that data protection and freedom of expression have been pitted against one another – see, for example, *Google Spain* – and finding a proportionate balance between the rights has not always been easy. The case is interesting in highlighting a unique and subtle approach to the interplay between the GDPR and the constitutional protection of freedom of expression in relation to credit information activity. The Swedish lawmaker clearly delineated the boundaries between the two rights by generally exempting certain publishing activities from the GDPR. At the same time, the legislator left the GDPR apply to apply in relation to specific ways to specific types of credit information activities.

Learn more

- UK Plans Big Tech Regulator -

According to the financial times, the UK is reportedly looking to set up a new regulatory body to supervise the activity of tech giants – such as Google and Facebook. The body will likely be set up next year following the completion of Brexit. The need for the body emerges on the back of twin recognitions. First, there is a substantive recognition that the behaviour of big tech companies – particularly in relation to the way these use individuals' personal data and in relation to their competition practises – needs close and specific supervision. Second, there is a structural recognition that, following Brexit, the UK will need to locally replicate regulatory competencies currently executed at European level – for example in relation to competition law regulation. It should be recalled, however, that the body remains only a proposal and several steps still need to be taken before the body becomes a reality. It should also be recalled that the final constitution and powers of the body will only crystalize later in the formation process. It will be interesting to see what the body finally looks like and whether it is endowed with the powers needed to fulfil its tasks. It will also be interesting to see how the body chooses to behave as a regulatory actor – which assumptions it will take as to the legitimacy of big tech and data processing, which regulatory models it will adopt as its own etc.

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.

Diana Dimitrova, Sub-editor: Researcher at FIZ


© FIZ Karlsruhe

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