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 9, 17 October 2019

- The CJEU gives Legal Certainty on Cookie Consent -

Last week, the CJEU decided another significant data protection case. The case concerned the operator of a lottery website in Germany – Planet49 GmbH – whose users' consent to analytics performed through cookies was collected via means of a pre-ticked box. The CJEU made four significant proclamations in the case. First, the CJEU implicitly indicated that consent is the only legal basis for operating cookies in accordance with the e-Privacy Directive. Second, the CJEU confirmed that consent may not be deemed to have been obtained in accordance with the GDPR and the e-Privacy Directive if users did not explicitly and actively give consent, e.g. by ticking a box. Third, the CJEU clarified that the preceding conclusion is not prejudiced by whether the storage or analysis of information through cookies qualifies as personal data: the purpose of Article 5(3) e-Privacy Directive is to protect the private sphere of users as defined by the ECHR and, in this case, there are privacy risks associated with the data stored on the terminal device of the end user regardless of the classification of data involved. Fourth, the CJEU clarified that the service provider must inform users about the duration of the operation of the cookies and whether any information is going to be disclosed to third parties. The implications of the ruling are significant, since many online service providers will now have to review and possibly adapt their consent collection practices. Interestingly – in par. 64 – the CJEU notes that the referring Court did NOT raise another important question: whether having to give consent to one's personal data being processed for advertising purposes as a prerequisite for taking part in the lottery would qualify as 'freely given' consent. Does this observation indicate that if a challenge were to be brought against the obligation to provide consent as a prerequisite to participate in the lottery, the CJEU would rule this to be forced consent?

Learn more

- EDPB Adopts Four Documents -

On October 8th and 9th, the EDPB met in plenary session. As a result of the session, the EDPB adopted the following four documents:

- A final version of the Guidelines on the lawful basis for processing for online services based on contracts (Art. 6 (1) (b))
- An opinion on the draft decision regarding Equinix Binding Corporate Rules (BCRs).
- A letter in response to MEP Sophie in't Veld's letter regarding the renegotiated draft PNR agreement with Canada and its impact on other PNR agreements.
- A response to the Council Working Party on Sports' request regarding the ongoing review process of the World Anti-Doping Code.

The documents are not yet available on the EDPB website. We would assume, however, that the documents will be made available over the course of the coming days and weeks following internal checks.

Learn more

- The Saga on LEA Access to Communication Data Continues -

Even though the political debate on the proposed e-Privacy Regulation is only now reviving, legal challenges to the existing e-Privacy Directive continue. On 15 October 2019 the CJEU will hold a hearing on three questions related to the interpretation of Article 15(1) e-Privacy Directive, including in light of the CFREU. First, the referring Court from Estonia asks whether LEA access to communication metadata should be restricted to "serious" crimes or whether access may also be extended to other crimes. Second, the Court seeks clarity concerning the proportionality of access and whether the amount of requested data may have some bearing on the legality of the interference – specifically, the Court seeks clarity on whether LEA requests to access smaller amounts of data may justify access in relation to less serious crimes. Third, the Court asks whether a prosecutor's office which initially leads the pre-trial procedure and is bound by independence, but which later represents the public prosecution in court, can be considered as an independent authority which may approve or refuse access to the data sought? This hearing follows a row of hearings on the access to telecommunications data by LEAs – as reported in previous editions of this newsletter. It remains to be seen how consistent the CJEU will be in its rulings across the different cases on Article 15 of the e-Privacy

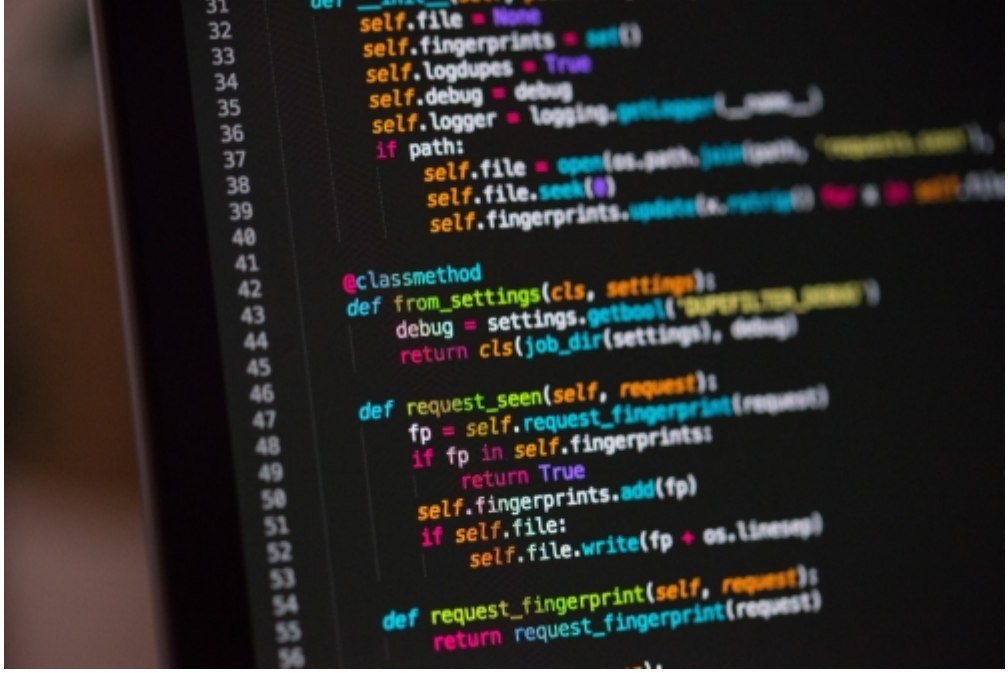
Directive as well as how concretely the CJEU will formulate answers to the questions asked. It also remains to be seen whether, and if so in what form, the results of these rulings will be included in drafts of the new e-Privacy Regulation.

Learn more

- Do European DPAs Have Sufficient Resources? -

The Irish DPA had requested a boost in its next annual budget, applying for almost an additional €6 million. The DPA only received, however, an additional €1.6 million. Despite the increase in the budget from last year, commissioner Helen Dixon indicated the extra resources are not enough to match the increase in DPA workload following from the entry into force of the GDPR. This increase in workload is partially due to the fact that the Irish DPA acts, in a number of cases, as the lead authority in cross border cases due to the fact that several large tech companies, such as Facebook, have chosen Ireland as their EU headquarters – this seems likely to increase post-Brexit. The news raises questions as to whether DPAs across the EU have sufficient resources, and accordingly, whether they can thus properly carry out and make use of their newly vested responsibilities and powers. These responsibilities and powers include not only responding to data subjects' complaints, requests for guidance and data breach notifications but also carrying out inspections and providing advice in legislative processes. The Irish Times also begs the question as to whether the reasons for the low increase in additional funding in this case are due to the recent decision of the DPA, in which it ruled that the State had illegally processed the data of those who own a public service card. Can DPAs work with full independence when the purse-strings are controller by data controllers?

Learn more



- Consent Chain Fraud in Ad-Tech -

Reporting this week brought the issue of consent chain fraud in ad-tech to the top of the agenda. Consent chains are used in ad-tech to demark the organisations and purposes for which a user has consented to their personal data being used. As user data moves through the ad-tech ecosystem, these consent chains are passed along with the data. Consent chain fraud occurs as ad-tech actors manipulate the consent strings in order that these strings appear to allow a broader scope of consent than that originally provided by the data subject. There remains little clarity as to how wide-spread the practise of consent chain fraud really is. Nevertheless, it seems likely an image of the scale of the issue will emerge as more work is done. Reporting on consent chain fraud is significant for at least two reasons. First, the ad-tech industry is already under heavy scrutiny. This scrutiny follows warnings given by DPAs that ad-tech practises may infringe the GDPR as well as follow-up warnings that efforts to change problematic practises have hitherto been inadequate. Reporting on the existence of consent chain fraud, at this point in time, will put further pressure on the industry. Second, consent chain fraud represents a deliberate organisational violation of data protection principles which has emerged, allegedly, on the back of the GDPR. Consent chain fraud is thus a fascinating instance of data protection law providing the specific conditions for organised entrepreneurial delinquency.

Learn more

- Study Shows Widespread Inadequacy in Data Access Restrictions -

A recent study by Sila Solutions Group and the Ponemon Institute has highlighted widespread inadequacies in internal access restrictions to personal data held by companies. Concerningly, 70% of respondents to the researchers suggested that staff within their organisations may be accessing sensitive personal data without a clear organisational reason. In this regard, the study suggests the cause of the problem is that companies struggle to outline subtle and scalable approaches to setting access privileges. On the one hand, the study primarily dealt with US companies and their practises. It is thus possible that differences in European organisational approaches as a result of the GDPR mean the results of the research are wholly inapplicable to European organisations. On the other hand, however, this seems unlikely to be the case for at least two reasons. First, there is already empirical work done highlighting the fact that many European companies are not fully compliant with the GDPR. Second, the problems highlighted in the survey emerge as a result of organisational imprecision in dealing with personal data. This is highly likely a shared feature of organisations on both sides of the Atlantic. It would nevertheless be interesting to conduct the same research with European organisations as the subjects of study.

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
