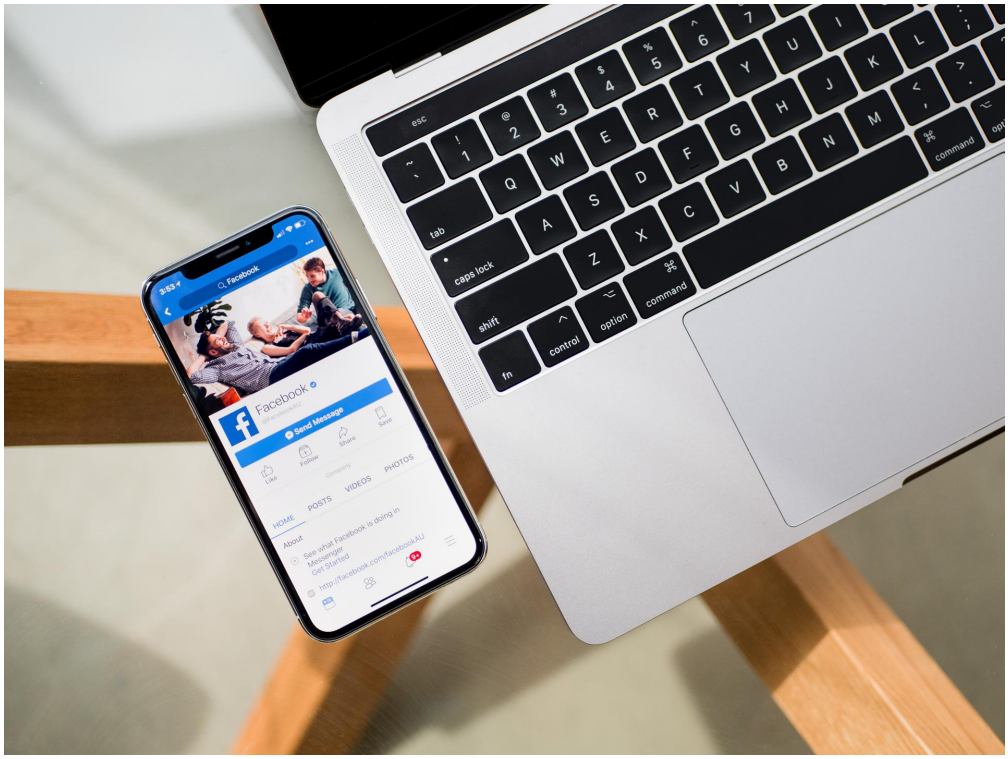
EDPL EUROPEAN DATA PROTECTION LAW REVIEW

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

Data Protection Insider

Issue 4, 08 August 2019



- CJEU Deals with "Like" Button in *Fashion ID* Judgment -

In the recent *Fashion ID* judgement concerning data protection responsibilities with regards to Facebook "like" buttons on websites, the CJEU ruled that websites embedding such social plug-ins are considered to be data controllers and likely require consent for the use of the plug-ins. This is a rich and varied case dealing with several significant issues. These include: the relationship between data protection and unfair commercial practises; the relationship between the GDPR and e-Privacy; the legitimacy of consumer organisations filing data protection complaints; the choice of legitimating ground; and the definitions of 'controller' and 'joint-controller'. Of particular note is the ruling of the Court that websites employing social media plug-ins only need to inform data subjects and gain their consent as regards the operations the website is responsible for. With this ruling, the Court thus leaves open the question of the legality of the subsequent processing of the data, harvested through the plug-in by the social media platform. This is an odd and confusing ruling. If the website deploying the plug-in is not responsible for collecting the consent of the user in relation to the further use of personal data by the social media platform, how should such further use ever be legitimated?

Learn more

- Not all Member States Transpose Police Directive -

The European Commission has referred Greece and Spain to the CJEU for failing to transpose Directive 2016/680 ("the Police Directive") into their national laws. The transposition deadline expired on May 6th, 2018. The Police Directive was adopted at the same time as the GDPR and seeks to harmonize the level of data protection in the field of law enforcement. Failing to transpose the Directive leads, on the one hand, to a lack of proper protection of the suspects, victims, witnesses, convicts, etc., whose data is processed in the law enforcement context. On the other hand, failure to transpose hampers the free exchange of personal data between the Member States' competent law enforcement authorities. In its action, the Commission has applied to both impose a lump sum fine as well as a daily penalty payment. The Commission's aim is to penalise both the existence and the continuation of the infringement.

Learn more

- Hamburg vs Google Smart Speakers -

Hamburg's DPA has ordered Google to stop further processing data collected by Google's digital personal assistant across the EU. The ban came after Google confirmed that its employees could hear parts of users' conversations without their consent. The DPA found such processing to be in breach of the GDPR. Google has confirmed that it has now stopped listening to the data it has collected. The ban is effective only for three months. The temporal limitation is in place as the Irish DPA – the DPA into whose jurisdiction Google falls – would be the lead authority in a full investigation under the one-stop-shop principle. The action taken by Hamburg is, however, likely to influence the further actions of the Irish DPA. Bearing in mind that Amazon has also confirmed it is listening to echo users' conversations, Hamburg's action has the potential to trigger a wave of bans and sanctions by other DPAs in relation to other companies engaged in similar activities. The ban may also have wide-ranging consequences for the (research) practices adopted by companies.

Learn more

- DPA Sanctions Accountability Violations -

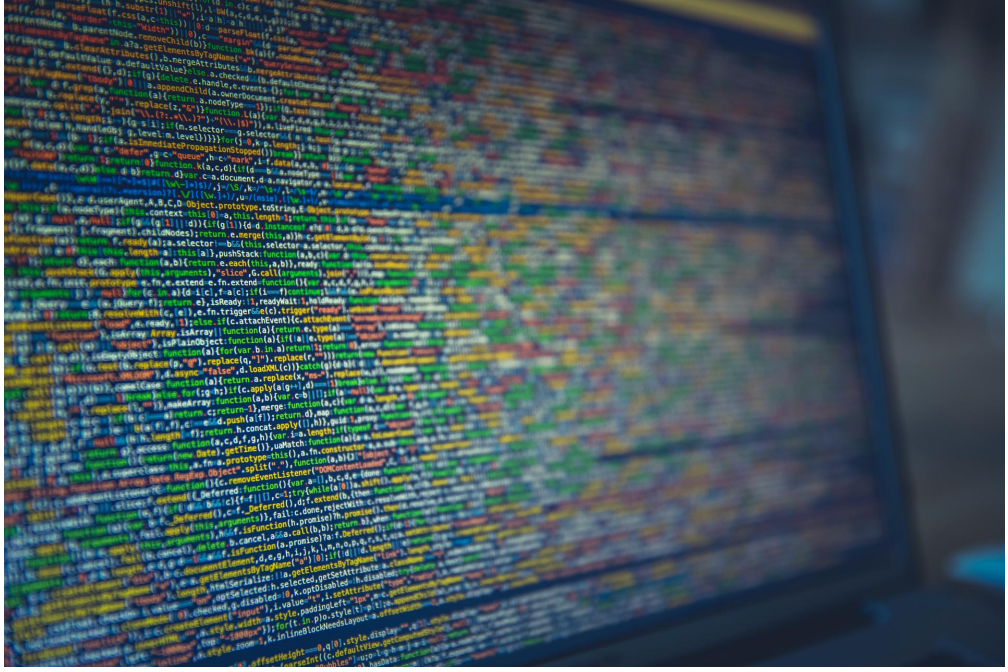
The Greek DPA has fined PricewaterhouseCoopers 150,000 EUR in relation to the illegitimate processing of employees' personal data. In terms of substance, the DPA took issue with three aspects of PricewaterhouseCoopers' processing. First, the DPA found that the use of consent to justify processing in employer-employee relations was illegitimate. Second, the DPA found that telling employees that consent was the basis for processing, when in fact the basis was the legitimate interests of the company, was unfair and intransparent. Finally, and most interestingly, the DPA found that PricewaterhouseCoopers' had failed to meet its obligations under the accountability principle in Article 5(2) GDPR. The DPA held that PricewaterhouseCoopers' had not only failed to provide adequate documentation to the DPA regarding the choice of legal basis but also that the company had illegitimately sought to transfer its data protection responsibilities – in particular the burden of proof of compliance – to employees. The decision represents, to our knowledge, the first instance in which a DPA has found violations of the accountability principle as grounds for handing down sanctions. In doing so, the decision specifically highlights accountability as 'the core of the compliance model' adopted by the GDPR.

Learn more

- New DPIA on Microsoft Office and Windows -

The Privacy Company have produced another DPIA dealing with Microsoft – this time dealing with 'Microsoft Windows 10 Enterprise, Office 365 ProPlus and Office Online, as well as the mobile Office apps'. The DPIA is significant for at least two reasons. First, the DPIA constitutes one of the few extensive DPIAs published since the GDPR's entry into force. Given the lack of clear guidance on how to effectively conduct a DPIA as well as the difficulty companies have had in meeting the DPIA obligation, it seems likely the procedural approach of the DPIA will have hortatory force. Second, the DPIA brings forward further criticisms of Microsoft products. In particular, the DPIA is critical of Office Online and mobile Office apps – although the DPIA was positive about other evaluated products. The DPIA specifically problematizes the fact that Microsoft sends user data to a marketing company in the US, which is not subject to the privacy safeguards binding Microsoft, 'without the user's knowledge and without any information about the presence or purpose of this processing'. The previous DPIA conducted by the Privacy Company on Microsoft was the subject of considerable debate in privacy communities and led to greater general scrutiny of the products it assessed. It would seem likely this DPIA will have a similar effect.

Learn more



- The Financial Cost of the GDPR -

Recent empirical research into the financial impact of European data protection law shows certain websites are making less money as a result of the GDPR. The research looked at the pre- and post-GDPR revenue for websites whose revenue streams include page views and those whose revenue streams include e-commerce. The research found that websites made 10% less money post-GDPR. There are certain caveats to the research. In particular, the scope of websites and business models analyzed was limited, the source data on analyzed websites was likely incomplete and there remains uncertainty as to whether the GDPR was indeed the causal factor in the reduction of earnings. Regardless of these caveats, such research results are significant. The results begin to populate the discussion of the impact of data protection on innovation and business with facts. The tension between the protection for data subjects and the promotion of business interests sits at the heart of the GDPR. Unfortunately, the debate as to the nature of, and correct balance between, these rights and interests has, to date, been highly polarized and empirically lacking.

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 Karlsruhe and PhD candidate at Vrije Universiteit

© FIZ Karlsruhe

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