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 6, 05 September 2019

- EU to Consider Facial Recognition Regulation -

The European Commission are considering putting together legislation dealing with the use of facial recognition technology. In an interview with the financial times, Commission representatives stated that the new legislation would give EU citizens the right to "know when [facial recognition] data is used" and would tightly circumscribe any exceptions. The announcement is not a surprise. It follows a surge in public, academic and legal interest in facial recognition technologies – for example, the ICO investigation into the use of facial recognition technology in King's Cross in London. It remains uncertain, however, whether such a legislative proposal will eventually come to fruition. It also remains uncertain as to what such legislation will look like in form and content. Perhaps the largest hurdle to overcome for such legislation will be the argument that adequate rules to protect individuals' rights potentially impacted by facial recognition technologies already exist under the GDPR. If this is found not to be the case – or at least argued strongly enough in relevant fora – a legislative proposal could arrive sooner rather than later.

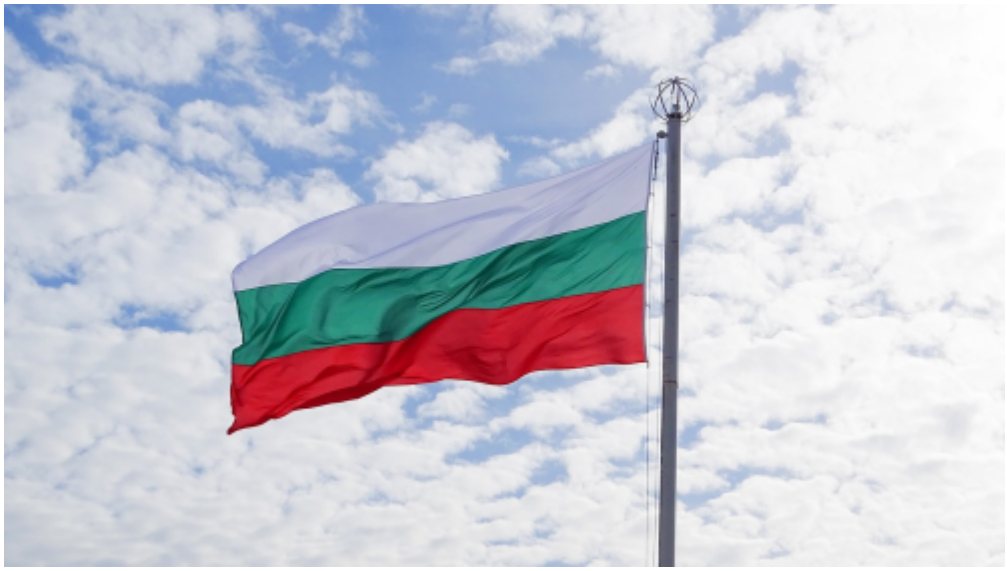
Learn more

- Bulk Communication Surveillance Hearings before the CJEU -

On 9th and 10th September, the CJEU will hold two preliminary ruling hearings on the topic of bulk communication surveillance for national security. The first hearing – relating to a case initiated by the Investigatory Powers Tribunal in the UK – concerns the scope of Union law. The case considers, in particular, two issues: 1. whether the requirements for bulk communication disclosure by a telecommunications operator to national security authorities falls within the scope of Directive 2002/58/EC and Union law; 2. whether the requirements on bulk surveillance established in the Watson case apply to bulk surveillance of telecommunications data. The second hearing – concerning joined cases initiated by the Conseil d'Etat in France – concerns the legality of bulk retention of telecommunication data under Directive 2002/58/EC and Directive 2000/31/EC in light of the CFREU. An interesting question raised in relation to the second hearing is whether, under Directive 2002/58/EC, the controller must notify the data subject of the surveillance where such notification would not jeopardize investigations. The answer to this question may have a significant impact on the information practices of national security authorities. These cases on bulk surveillance fall within a line of similar cases recently heard before the

ECtHR. The topic of bulk surveillance has been largely dormant of late. With the upcoming rulings, however, the legality of bulk surveillance will be clarified and the topic will likely reemerge as a subject of discussion.

Learn more



- Bulgarian DPA Issues Multi-Million Euro Fine -

The Bulgarian DPA has issued a fine of 5.1 Million Bulgarian Lev (approximately 2.6 Million Euros) to the Bulgarian Tax Authority. The fine relates to an incident in which hackers accessed Tax Authority systems and obtained Bulgarian citizens' tax information. Information on most of the Bulgarian population was obtained in the incident. The DPA assert that the incident was the result of inadequate information security measures in place at the Tax Authority. The Tax Authority maintains the imposition of the fine was unjustified and have suggested they will appeal the decision. One of the most interesting aspects of this case is the size of the fine. In previous issues of Data Protection Insider, we have paid close attention to the scale of sanctions issued by DPAs – as a key driver of data controller thought and action in relation to the GDPR. In particular, we remarked on a nascent disparity between sanctions in Eastern and Western Europe. This decision marks the first time a DPA in Eastern Europe has issued a fine in the millions of Euros. The sanction falls far short of top-level Western European sanctions – which stretch into the tens-of-millions. Nevertheless, the sanction constitutes a marked move toward greater parity.

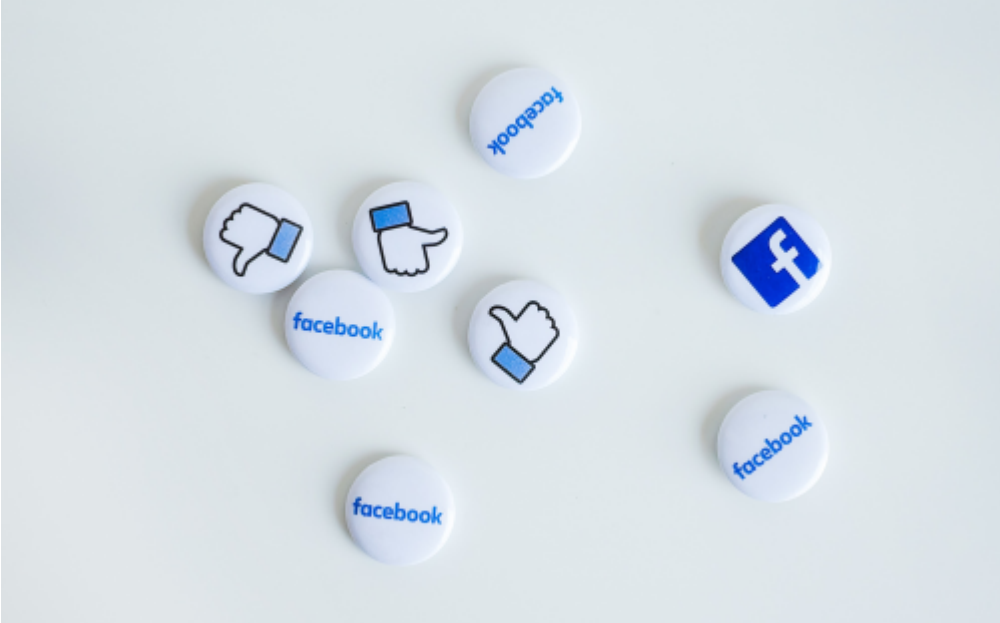
Learn more

- Biometric Pilot Results in First Swedish Fine -

A Swedish municipality has carried out a pilot programme using facial recognition technology to monitor students' attendance at school. In carrying out the pilot, the authorities attempted to legitimate data processing by obtaining the consent of the students. The Swedish DPA, however, ruled that consent cannot constitute a valid legal basis in the case owing to the clear power imbalance between the controller and the data subjects. In addition, the DPA ruled that the processing of sensitive biometric data was carried out without a Data Protection Impact Assessment. On the back of the ruling, the DPA decided to impose a fine of approximately 20,000 Euros. The DPA's reasoning in the case is significant for several reasons. First, the decision highlights that consent, in pilot projects involving power imbalances, cannot be assumed to be freely given. If this reasoning is followed by other DPAs, many research projects involving actors engaging similar concerns may have to re-consider the legal basis on which they collect and process personal data. For instance, to what extent can research projects carried out with the participation of law-enforcement authorities assume consent to be freely given? Second, this decision represents the first time, to our knowledge, that a DPA has handed down a fine for a missing or inadequate Data Protection Impact

Assessment. Finally, the decision deals with a small-scale pilot project. Such projects often regard themselves as irrelevant to DPAs and unlikely to be fined. This decision shows that this is not necessarily the case.

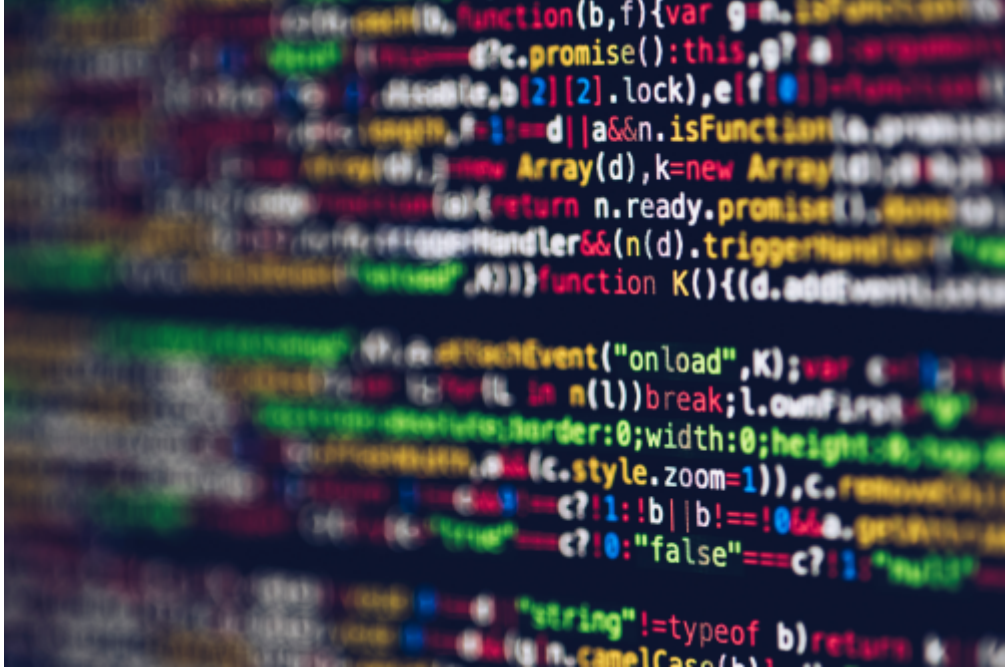
Learn more



- Facebook, Data Protection and Competition Law? -

The German Federal Cartel Office (FCO) recently issued an order against Facebook to stop collecting user data across its platforms. The order followed the FCO's conclusion that Facebook's practices of gathering users' data across its platforms, without consent, breached competition law. However, the Higher Regional Court in Düsseldorf has suspended the order. The Court argued that, whilst the data gathering practices could be considered to breach data protection law, these practices did not automatically infringe competition law. Accordingly, the Court neither found an abuse of the dominant position Facebook holds, nor did it find an exclusionary abuse. The Court poignantly pointed out that the FCO did not seek to prevent the data collection practices per se, but required user consent instead. However, in the view of the Court, user consent may not be relied on to rectify or prevent competition law breaches. The FCO will appeal the ruling before the German Federal Court of Justice. The case highlights interesting questions concerning the boundaries between, and interaction of, data protection and competition law. For example, to what degree can practices which can be considered legal under data protection laws, e.g. processing with valid consent, still be found to be breach of competition law?

Learn more



- ICO Receive Inadequate Response from Adtech -

Approximately two months ago, the ICO warned the Adtech industry their practises were in contravention of data protection law. On the back of this warning, the ICO gave the industry a six-month window in which to address problems – including failure to obtain explicit consent for the processing of sensitive data. In an interview with the Financial Times, the ICO have offered a scathing update on the review process. Simon McDougall, the ICO's lead investigator stated that 'absolutely nothing has been solved or resolved at this point' and that the industry has only provided 'vague, immature and short answers'. The ICO investigation runs in parallel with other investigations into Adtech practises in Europe – notably an investigation carried out by the Irish Data Protection Authority. If these investigations are carried through to their conclusions, they will likely have significant repercussions for Adtech, and thereby the internet as a whole. Doubts have been expressed as to whether a happy consensus can be found between data protection law and the current manifestation of Adtech. Data protection law functions by ensuring citizens have transparency and control over their personal data. Key mechanisms in Adtech, however, allegedly function in ways which mean provision of meaningful information to citizens as to where their data will go and what it will be used for, could be very difficult.

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 also programme

© FIZ Karlsruhe

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

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu
