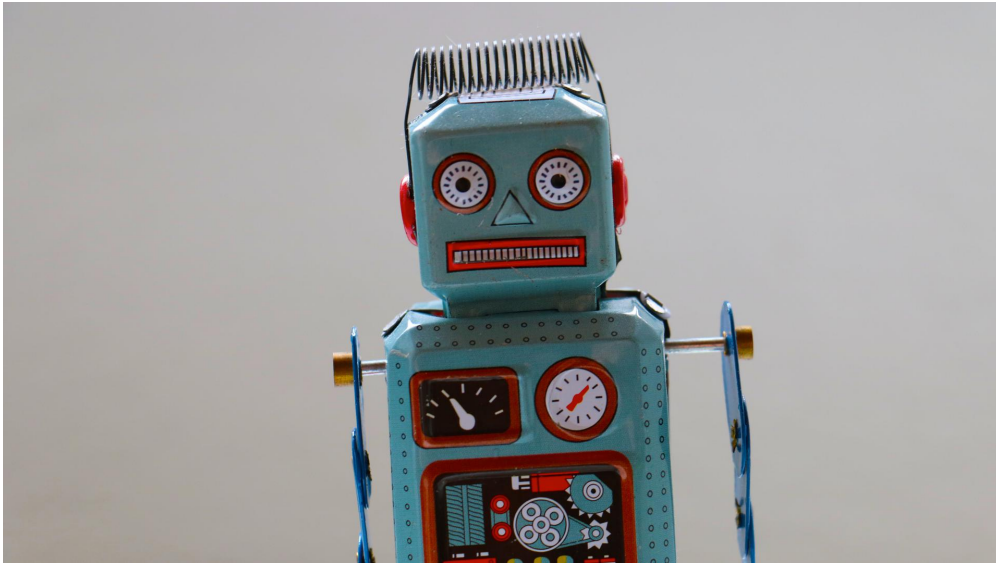# Data Protection Insider

Issue 2, 8 July 2019

- New AI-HLEG Report on Trustworthy AI -

The EU High-Level Expert Group on AI has released its second report: Policy and Investment Recommendations for Trustworthy AI. In the words of the group, the 'document…presents a set of policy and investment recommendations on how Trustworthy AI can actually be developed, deployed, fostered and scaled in Europe, all the while maximising its benefits whilst minimising and preventing its risks'. The proposal contains **several suggestions for EU institutions and Member States**. One particularly noteworthy suggestion is that a 'risk-based' approach to AI regulation be adopted. The report is significant owing both to the institutional support for the group as well as to the prominence of the members of the group. The content of the group's work has hitherto, however, not gone without criticism. It will be interesting to see how the present report is received.

Learn more
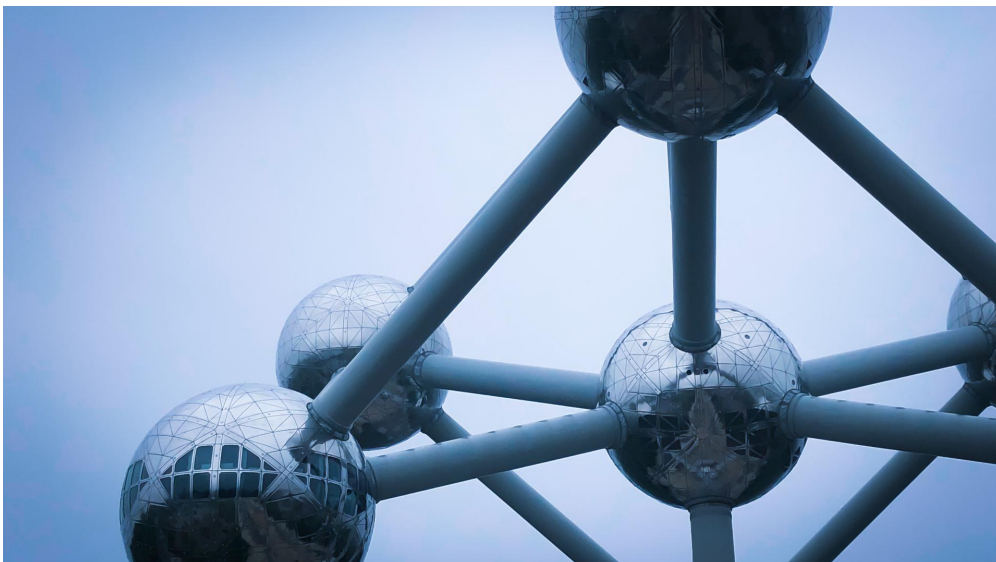
- E-Privacy Regulation Proceeds before the Council -

The EU Council has resumed work on the proposed E-Privacy Regulation. On the 27th of June, the Finnish Presidency opened a consultation to Member States on the Regulation. This consultation preceded a policy meeting on the 4th June. The consultation invitation requested **broad feedback on the proposed Regulation**. Feedback encompassed opinions on which parts of the Regulation are most essential, which parts which are most problematic and which parts are not necessary at all. At first sight, the consultation and meeting appear minor procedural developments. The E-Privacy Regulation, however, is often forgotten in EU data protection discussions. This is not surprising, given its painfully slow and opaque progression through the institutions. News that the proposal is alive and well, and that discussions are ongoing, is therefore welcome.

<div style="background:yellow">Learn more</div>
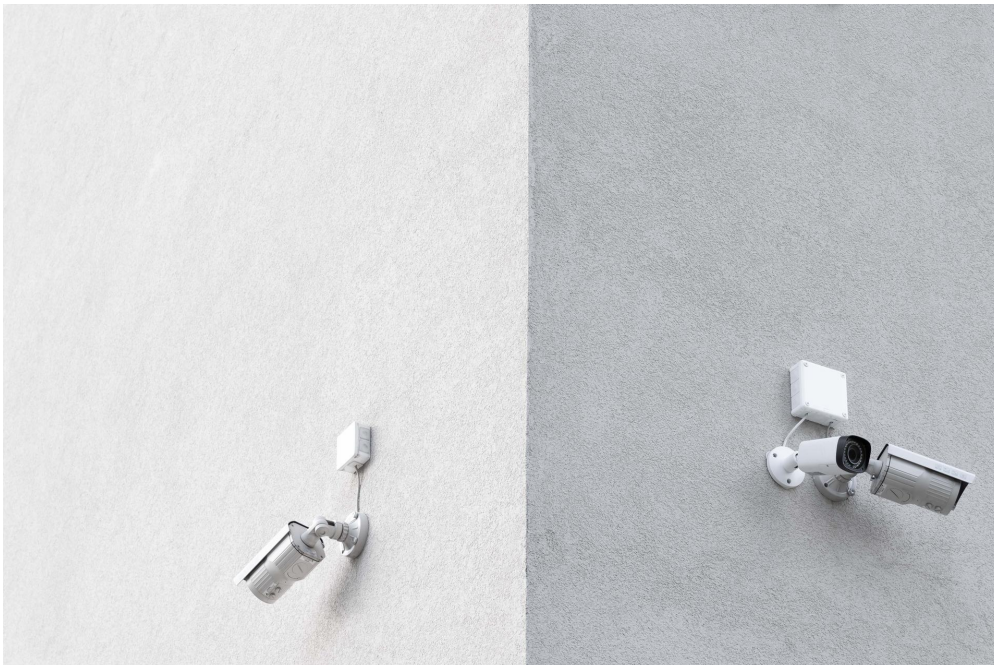
- ECtHR Rules on Prisoner CCTV Surveillance -

In the *Gorlov and others v Russia* case, the European Court of Human Rights (ECtHR) ruled on the question of permanent CCTV surveillance of prisoners in Russia. The Court concluded a violation of Article 8 on the basis that relevant Russian law failed to respect quality of the law requirements under the ECtHR. The Court highlighted flaws in the law owing to lack of specification of 'whether the obtaining of such information is limited to monitoring by CCTV cameras…whether that information is recorded and kept…what the applicable safeguards and rules are governing the circumstances in which such data may be collected, the duration of their storage, the grounds for their use, and the circumstances in which they may be destroyed'. After finding a breach of the quality of the law requirement, the Court did not examine questions of necessity and proportionality of CCTV surveillance either in prisons or in general. **This judgment continues a trend in ECtHR case-law** ruling on data processing and surveillance cases via quality of law considerations. This may be disappointing to some in the data protection community who would

welcome clear substantive conclusions from Strasbourg on legitimate and illegitimate surveillance.

Learn more

- British Airways Faces Huge Data Breach Fine -

On the 8th of July, the Information Commissioner's Office (ICO), the British data protection supervisory authority, issued its intention to fine British Airways £183.39M for a data breach. According to the ICO, the incident involved 'user traffic to the British Airways website being diverted to a fraudulent site' and impacted the personal data of roughly 500,000 of BA's customers. The ICO regard the breach to have resulted from the inadequate security arrangements put in place by British Airways. This scale of the fine is highly significant. Empirical research shows **the main driver behind compliance with the GDPR is the scale of potential DPA fines**

– up to 20,000,000 Euros or 4% of annual turnover. Up to now, however, there had been little indication that DPAs were willing to use the full force of their new sanctioning powers. This case highlights – at least in the UK – that there should be no assumption that DPAs will be lenient or that there are unwritten restrictions on the scale of fines to be handed down. The fine is not final and British Airways may still appeal.

[**Learn more**]

- Facebook Fined in relation with Cambridge Analytica -

The Italian Data Protection Authority, the Garante, has fined Facebook € 1M in relation to the Cambridge Analytical Scandal. The fine was imposed in connection with the ThisIsYourDigitalLife app. The app, which was connected with Cambridge Analytica, was downloaded by almost 60 Italians and harvested the data of about 200,000 Italians without consent. Since the infringement took place before the entry into force of the GDPR, the calculation of the fine follows the old provisions on fines – fines under these provisions are considerably smaller than those allowed by the GDPR. This is **another significant movement toward the development of data protection as a legal instrument** for the protection of voters and for the legitimate conduct of profiling in election campaigns. In the same week, Germany also fined Facebook €2M for violating German laws on combating hate speech online. This fine was imposed based on Facebook's failure to submit complete information on the number of complaints received concerning unlawful content.

[**Learn more**]

- Schrems vs Facebook: Update -

The court battle, initiated by Max Schrems, over the legality and fundamental rights compliance of Standard Contractual Clauses (SCC) and Privacy Shield – relied on for transfers of personal data by Facebook, and other companies, to the US – continues. On the 9th of July, the case advanced to the CJEU in the form of a preliminary hearing. The current case is a follow-on from the 2015 CJEU case concerning **Facebook transfers to the USA on the basis of the Safe Harbor framework**. Under this previous case, the Safe Harbor framework was struck down by the CJEU on the basis that it did not provide adequate protection for EU citizens' personal data stored in the US – largely as it allowed, without procedural guarantees, bulk access by US intelligence services to all EU personal data. Although this previous case did not concern SCCs, there have been no material changes to the SCC framework since the 2015 case and their legality, accordingly, seems precarious. Although Privacy Shield was intended as a replacement for Safe Harbor following the 2015 case, criticism has been voiced that substantive issues remain unaddressed.

[**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 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.

© FIZ Karlsruhe

Learn more about EDPL

Image

Terms | Privacy