Reports

This part of the EDPL hosts reports in which our correspondents keep readers abreast of various national data protection developments in Europe, as well as on the most recent questions in different privacy policy areas. The Reports are organised in cooperation with the Institute of European Media Law (EMR) in Saarbrücken (www.emr-sb.de) of which the Reports Editor Mark D. Cole is Director for Academic Affairs. If you are interested in contributing or would like to comment, please contact him at mark.cole@uni.lu.

Recent Developments and Overview of the Country and Practitioners Reports

*Mark D Cole and Christina Etteldorf**

On 25 May, the GDPR celebrated its fourth birthday since being applicable. A lot has happened in data protection law in these four years. What can be concluded in any case, without having to resort to statistics, is that the GDPR has raised awareness of data protection and privacy – both on the part of data subjects, who have become aware of their rights, and on the part of data processors in the private and public sectors, who have had to become mindful of their compliance obligations. This in turn has resulted in authorities and courts also becoming (more) active in enforcing data protection rights and obligations. And this one can indeed show also with statistics.

A look at one of the (unofficial) 'enforcement trackers'[1] reveals concrete figures for this, at least in the area of administrative fines. Based on that data, in total 1.111 fines amounting to 1,644,519,546 euros (as of June 2022) were imposed. Two things are particularly noteworthy when taking a closer look at these figures in terms of numbers and content: While initially (2018/2019) fines were imposed relatively cautiously (on average 9 per month), this then (2020/2021) increased rapidly (on average 33 fines per month) and now (2022) seems to have settled (also 33 fines per month on average so far), although it remains to be seen whether this will also remain constant in the fifth year of GDPR. The developments in the amounts of fines are similar. On the other hand, the authorities are "venturing" more and more into "new technological realms", devoting themselves to topics that have so far been only examined to a limited extent from the perspective of data protection law. For example, the Hungarian data protection authority recently imposed a fine of about 250 million forints (~650,000 euros) on the Budapest Bank for using "emotional AI" – which evaluated customer calls on the basis of voice timbre and volume, for example, and assigned the calls to a category (possibly according to urgency or degree of dissatisfaction), which then decided on the human recall (or the decision not to call back, probably).[2] The Icelandic data protection authority fined the municipality of Reykjavík 5,000,000 ISK (~36,000 euros) for the use of the Seesaw educational system – an interactive learning platform for elementary schools.[3] Increasingly, the big US tech players are also being targeted by investigations and sanctions – even outside of measures taken by the lead Irish supervisory authority, as illustrated by the recent fine from Spain (among many others across Europe) imposed on Google LLC (note: not Google Ireland Ltd.) for the

DOI: 10.21552/edpl/2022/2/11

* Mark D Cole, Professor at the University of Luxembourg, Director for Academic Affairs, EMR, and EDPL Associate Editor. For correspondence: <mark.cole@uni.lu>. Christina Etteldorf, Senior Research Scientist at the EMR and lecturer at the University of Saarland. For correspondence: <c.etteldorf@emr-sb.de>.

1 CMS, 'enforcement tracker – Fines statistics', https://www.enforcementtracker.com/?insights (as of 5 June 2022).

2 NAIH, decision NAIH-85-3/2022, https://naih.hu//hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei (8 February 2022).

3 PV, decision no. 2021040879, https://www.personuvernd.is/urlausnir/notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur-sektarakvordun-1 (6 May 2022).

amount of 10,000,000 euros for unlawfully transferring personal data to a third party and for impeding the exercise of the right to erasure.[4]

This picture is also confirmed by more frequently published activity reports from national authorities. For example, the activity report of the French data protection authority for 2021 documents a significant rise in complaints, sanctions, inspections and notifications of data protection violations and a record amount in the total amount of fines (over 214, 000, 000 euros). The two most prominent issues were the use of cookies (one of the larger fines against the company Amazon in such a matter was just recently confirmed France's Council of State in light of questions around the One-Stop-Shop mechanisms)[5] and the processing of health data in the context of the pandemic.[6] The European Data Protection Board (EDPB) has also published its activity report for 2021 which gives us a broader impression of the developments in the EU.[7] With regard to law enforcement that report particularly highlights the EDPB's very first Art. 66 GDPR Urgent Binding Decision following a request from the Hamburg supervisory authority, which had adopted provisional measures against Facebook Ireland ltd., as well as its second Art. 65 GDPR binding decision which sought to address the lack of consensus on certain aspects of a draft decision issued by the Irish authority, acting as lead supervisory authority, regarding WhatsApp Ireland Ltd, both dating from July 2021.

Other main areas of activity were digital policy and, first and foremost, international transfers of personal data particularly in the aftermath of the Schrems II ruling by the Court of Justice of the EU. The Recommendations on supplementary measures following Schrems II, adopted by the EDPB in 2021[8], may soon have to be read in the context of new developments, at least when it comes to data transfers to the US. As already mentioned in the introduction of the last issue of EDPL, the negotiations between the EU and the US for a "Privacy Shield 2.0" are becoming more concrete. The EDPB also commented on this in a statement in April 2022[9]: Although the Board welcomes the commitments made by the U.S. to take 'unprecedented' measures to protect the privacy and personal data of individuals in the European Economic Area in general, it notes that this announcement does not constitute a legal framework on data transfers and that the "EDPB looks forward to assessing carefully the improvements that the new framework may bring in light of EU law, CJEU case law and previous recommendations of the Board, once the EDPB receives all supporting documents from the European Commission" while already addressing key points for this assessment (eg. principles of purpose limitation and proportionality in pursuing national security purposes, data access of authorities, judicial remedy, etc.). Maximilian Schrems, the lead plaintiff in the "Schrems I" and "Schrems II" cases, on the other hand, found much clearer words on this subject matter in an open letter dated two days before GDPR's fourth birthday "warn[ing] negotiators on both sides of the Atlantic, the Council of the EU, the EDPB and the LIBE Committee of the European Parliament that the announced framework risks sharing the same fate as its two predecessors in front of the CJEU unless substantive (legislative) reforms are conducted in the United States"[10]. The letter addresses particularly three cornerstones of any future data transfer framework (applying a correct proportionality test on US surveillance law under Article 8 EU Charter of Fundamental Rights (CFR); creating meaningful judicial redress under Article 47 CFR; taking into account the need to update commercial privacy protections) in detail.

The activity report of the EDPB further lists for 2021 8 guidelines and recommendations adopted on topics such as personal data breach notifications, connected vehicles and virtual voice assistants, as well as 6 guidelines and recommendations in their final

4 AEPD, Expediente Nº: PS/00140/2020, https://www.aepd.es/es/documento/ps-00140-2020.pdf (18 May 2022).

5 CNIL, 'Cookies: the Council of State confirms the 2020 sanction imposed by the CNIL against Amazon', https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon (28 June 2022).

6 CNIL, 'Rapport annuel 2021', https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf (2022).

7 EDPB, 'Annual Report 2021: Enhancing the depth and breadth of data protection', https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2021 (12 May 2022).

8 EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, (18 June 2021).

9 EDPB, 'Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework', https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-012022-announcement-agreement-principle-new-trans_en, (6 April 2022).

10 Open Letter on the Future of EU-US Data Transfers, https://noyb.eu/en/open-letter-future-eu-us-data-transfers, (23 May 2022).

version following public consultation. This statistic does not yet include the most recent activities of the EDPB in 2022 which are highly interesting as well. During its May 4th plenary, the EDPB adopted an EDPB-EDPS Joint Opinion on the proposed Data Act[11] and during its May 12th plenary inter alia guidelines on the use of facial recognition technology in the area of law enforcement[12] and guidelines on the calculation of administrative fines under the GDPR[13] were decided. The latter in particular could contribute to (even) more consistency within the territorial reach of the GDPR when imposing fines in the future.

Another recent guideline concerns dark patterns in social media platform interfaces. These Guidelines are aimed to offer practical recommendations to designers and users of social media platforms on how to assess and avoid so-called "dark patterns" (ie specific designs of an interface that are intended to induce users to make a decision (e.g. purchase a product, give consent) that they would not have made on the basis of rational facts without being influenced) in social media that infringe on GDPR requirements by listing several common dark patterns (such as 'overloading', 'stirring', 'too many options', 'look over there', 'Deceptive snugness', etc.) and assessing them in light of data protection law.

A rule that addresses one of these dark patterns, namely that of "continious prompting" in the wording of the EDPB, can also be found in the Digital Markets Act (DMA)-Regulation, the final scope of which was agreed upon by the European Parliament and the Council on 24 March in the Trilogue and is up for vote in the EP Plenary beginning of July.[14] Art. 5(2) DMA prohibits gatekeepers to repeat their request for consent for the same purpose more than once within a period of one year in the context of several data merging activities. This prompted us to contribute an EMR-"in-house" report in which one of the undersigning authors, *Christina Etteldorf,* deals with the relationship between the DMA and current data protection law, in particular the GDPR, asking '**DMA – Digital Markets Act or Data Markets Act?**'. The contribution takes a look at the "data-relevant" provisions of the new Gatekeeper Regulation and raises questions about future coherence and consistency, the practical answers to which, however, will remain to be seen in the future.

Not only is the directly data protection/data flow regulatory framework expanded through recent proposals by the Commission but it is also being supplemented by not specifically data-oriented pieces of law such as the DMA that have a significant impact. Beyond that, the regulation of technology today typically - when connected to any type of online dissemination – is closely related to use of data and therefore rules on online services have always at least some impact on the legislative framework relating to data. How important it is to keep these developments "on the radar" of data protection-interested persons is clearly shown by *Teresa Quintel* that reports in her contribution '**The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?**' Her report focuses on a legislative proposal for a Regulation laying down rules to prevent and combat child sexual abuse. Although it seemingly deals with a very different aspect than data use, in the proposed version includes rules that could question some certainties of current legislation when it comes to data protection as it addresses obligations of service providers to contribute to acting against child sexual abuse material that is disseminated via their services by e.g. detecting and then reporting the existence of such material and removing or disabling access to it. Not only the substantive rules proposed herein pose questions, but also the institutional setup and cooperation between very different authorities and agencies needs to be carefully assessed in order to understand the potential implications, as *Teresa Quintel* demonstrates.

Another proposed new EU Act is assessed in the report of *Elisabeth Steindl* but taking a view from the perspective of practitioners and therefore integrated in our Practitioner's Corner. The report '**Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in light of the**

11 EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en, (4 May 2022).

12 EDPB, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement', https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

13 EDPB, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en.

14 Similarly, dark patterns are also included as prohibited form of behaviour in the compromise text for the Digital Services Act (DSA)-Regulation in the (preliminary numbered) Art. 23a.

Draft AI Act and its Interplay with the GDPR' examines the European Commission's first attempt to address emotion recognition systems de lege ferenda by analysing the effect the draft AI Act would have on the regulation of emotion technology and pointing out concerns about potential shortcomings. It also touches upon the interplay between the AI Act and the GDPR. Unlike for the above-mentioned DMA, potential ambiguities, inconsistencies and shortcomings can still be resolved in the course of the legislative process for the AI Act.

Besides these European level, as always we also take not of important national developments in the Reports Section of the EDPL. We are happy to provide you with insights from Bosnia-Herzegovina, Ireland, Portugal, Norway, the UK and Turkey from a variety of different angles.

As regular readers will know, over the course of the last four years we had country experts reporting about the national attempts at bringing in line with the new EU regulatory framework their national data protection law in our GDPR implementation series. In this edition *Milica Sikimić* now introduces us to a legal landscape of an EU-neighbouring country. In her contribution '**The GDPR Implementation in Non-Member States of the European Union: The Case of Bosnia-Herzegovina**' she reports on current legal and practical GDPR compliance in Bosnia and Herzegovina. The report emphasises the GDPR application in practice – the attitudes and views of entities that work directly with the data which are essential to protect, as well good practice of certain entities – reflecting how the GDPR is "implemented" in this country, the issues of priority and harmonisation between the GDPR and domestic legislation, and the advantages brought by application of the GDPR rules, not last to the companies that work and cooperate with EU-based undertakings.

While Bosnia-Herzegovina is striving to find its way to the GDPR, another now non-EU member may soon go its own way with its own approaches to data protection law after having so far been bound by the GDPR-rules as "Ex"-EU Member State: *Irith Kist* reports in her contribution '**Proposal for a New Data Regime in the UK: An Avenue to be Explored by the EU**' on the status of proposed changes to data protection law in the UK and the UK National Data Strategy focussing in particular on the impact of the UK approaches on scientific research. From that perspective, she argues, that some lessons can also be learnt from the national application in the UK. The report does so by shedding light on the implementation of the GDPR in the Netherlands concerning the use of data for research purposes and how proposed amendments in the UK are an avenue to be explored by the EU with potential benefits for this area.

A final non-EU-Member State perspective is offered by *Leyla Keser Berber* and *Ayça Atabey* who give us an important update on developments concerning the question of cross-border data transfer in Turkey and how this is impacted not only by the GDPR but (should) also be regulated in light of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In their contribution '**Evaluation of the Recent Developments in Laws and Policies Relating to Cross-Border Data Transfers in Turkey**' they show the deficiencies of a decision of the Turkish Data Protection Board which disregards the relevance of the Council of Europe's Convention when it comes to international data transfers in Turkey. They show how the limitation of interpretation of the Turkish data protection law without this consideration received not only much attention, but also criticism. The authors give the necessary overview of the existing legal framework in Turkey and argue for an improved understanding and application of the international norms to make national law function better in practical terms and considering the technological reality involving cross-border data transfers.

Three decisions by data protection authorities, of EU Member States complete this edition. One of the DPAs in an EU Member State is constantly under scrutiny by other DPAs and also the data protection community due to its relevance in supervising the big tech companies involved in large scale data processing of users in the EU. The Irish DPA is regularly lead DPA when it comes to online platforms and the assessment of their GDPR compliance. *Andrés Chomczyk Penedo* takes a close look in his report '**Can a Data Breach be Caused by Poor Quality Data? An Analysis of a Decision by the Irish Data Protection Commission and its Potential Influence on Future Financial Data Sharing**' on a very recent decision by the Irish Data Protection Commission. It gives some interesting insight on the approach chosen concerning the notions of data quality and data security when sharing data in the financial services industry. The author comments the decision in light of the upcom-

ing rules on EU level striving to establish a framework for the EU financial data space – one of the many "data spaces" that the Commission will be addressing as part of the data strategy – and shows how the understanding expressed in the Irish DPA's decision could impact the overall understanding of these concepts specifically in the financial industry.

The regulation of online advertising is increasingly being addressed on EU level and once again, it will be DMA and DSA changing the way this type of advertising can be rolled out and offered in future. But also national authorities, including data protection supervisory authorities, have been dealing with advertising online as this involves significant amounts of data processing in order to adapt the advertising to specific users. Numerous practices have been identified as being in breach of data protection rules in the past and we covered several of these decisions over the last years in the reports section of EDPL. In *Graça Canto Moniz* flash news report titled **'The Portuguese DPA's 'To Do' List for Unsolicited Marketing'** the author demonstrates the relevance of guidance notes of DPAs which – albeit not being legally binding – attempt at giving clear indications as to how companies can reach compliance in certain areas. In the guidelines of the Portuguese DPA this assistance is offered to providers of marketing actions towards users that are not in a commercial relationship with that company so far or have not consented to the marketing. This is an indication that not only reading and observing EU law and the national legislative framework, but also taking into account guidelines and other expressions by the national DPAs, e.g. in annual reports, can be an important approach for companies to avoid risking fines for non-compliance.

The contribution from Norway by *Lara Marie Nicole Eguia* also deals with the processing of data for advertising purposes but within another context and in light of especially sensitive data concerned. She reports on the decision of the Norwegian supervisory authority (Datatilsynet) in the so-called Grindr case, which has also received a lot of attention outside Norway. In her contribution '**Snatched up by Advertising Partners: Norwegian DPA Fines Grindr for Lack of Consent over Third-Party Data Sharing**' she gives us an overview on the decision of Datatilsynet which resulted in a 6,500,000 Euro administrative fine against the dating app which is popular in the LGBTQ+ community. The authority not only concluded that Grindr lacked the legal basis to share the personal data of its users to third parties for online behavioural advertising purposes but also elaborated on the fact that the data breaches were particularly serious in this case because they concerned special categories of personal data including data on sexual orientation the disclosure of which could lead to discrimination and other serious harms for the data subjects. Against this background the author underlines the importance of ensuring that data on individuals' sexual orientation is handled with utmost care, putting great weight on the protection of the fundamental right to privacy, in light of the stigma that unfortunately still surrounds LGBTQ+ persons.

This overview of our reports once again demonstrates the diversity of topics and developments that we can cover thanks to our Country Experts. We, the Editors together with the Institute of European Media Law (EMR), hope to have made a worthwhile selection in sharing with you these reports and are sure that they will prove useful to you. We invite you to continue to suggest reports on future national and European developments to us. To submit a report or to share a comment please reach out to us at <mark.cole@uni.lu> or <c.etteldorf@emr-sb.de>.