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 Practitioner's Reports

*Mark D Cole**

Now that we are three years into applicability of the GDPR, it seems that the parties involved in the monitoring of compliance and enforcement have come 'into the groove' to speak musically. Hardly a week goes by without news about relevant decisions by data protection authorities and courts. With four decisions on 12 May 2021, the Luxembourgish *Commission nationale pour la protection des données* has completed the line of national data protection watchdogs making use of their power to issue fines. Each of those cases[1] concerned breaches of data protection law (Art. 5(1)(c) GDPR) by video surveillance measures in different constellations. The overall punishment was €7,900 (€1,000, €2,600, €2,400 and €1,900 respectively) and relatively modest, but adding to an overall volume of fines of all DPAs since applicability of the GDPR to nearly 300 Million Euro according to a source adding all individual fines.[2] However, the more decisions are made, the more important the consistency and coherence of the application of data protection law becomes, and the more decisions that are of cross-border relevance or concerning companies operating across borders, the more jurisdictional questions arise. With regard to the former, the EDPB is very active as the forum for cooperation between national data protection authorities. Not only with the publication of a leaflet on the question "How does the EDPB ensure harmonised data protection rights across 30 countries?"[3], which among other things explains the one-stop-shop mechanism for a general audience in simple terms, but above all with a series of new Recommendations (for example on data transfer tools and on the justification of storing credit card information), Guidelines (for example on the targeting of social media users and on the application of Art. 65(1)(a)) and Joint Opinions (for example on the issue of Artificial Intelligence or on Standard Contractual Clauses).[4] Consequently, two contributions of this edition's Reports Section deal with the EDPB's positions.

Laura Drechsler reports in her contribution "**EDPB Issues Guidance on Personal Data Transfers Based on Adequacy Decisions in the Context of the Law Enforcement**" on the EDPB's approach on personal data transfers based on adequacy decisions. She fo-

DOI: 10.21552/edpl/2021/2/10

* Mark D Cole, Professor at the University of Luxembourg, Director for Academic Affairs, EMR, and EDPL Associate Editor. For correspondence: <mark.cole@uni.lu>.

1 Délibération n° 14FR/2021, <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-14FR-2021-sous-forme-anonymisee.pdf>; Délibération n° 15FR/2021, <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-15FR-2021-sous-forme-anonymisee.pdf>; Délibération n° 17FR/2021, <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-17FR-2021-sous-forme-anonymisee.pdf>; Délibération n° 16FR/2021, <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-16FR-2021-sous-forme-anonymisee.pdf>.

2 Exactly €293.830.537 as of 29th July 2021, according to the GDPR fine tracker available at <https://www.privacyaffairs.com/gdpr-fines/>.

3 See, <https://edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf>.

4 See for an overview <https://edpb.europa.eu/our-work-tools/documents/our-documents_en>.

cusses in particular on the Recommendation on the adequacy referential under the Law Enforcement Directive and the Opinion on the European Commission Draft Implementing Decision on the adequate protection of personal data in the UK. Looking at the Law Enforcement Directive is not only relevant due to the Recommendation but also because the LED has received much less attention in its practical application so far compared with the GDPR. She points out that the EDPB, while being rather hesitant in its critique of the approach to the question of adequacy of protection standards in the UK, nevertheless raises several important points which can also be fruitful for any future occasion of LED adequacy decisions. The transnational context of data protection is also the topic of *Carl Vander Maelen's* report "**First of Many? First GDPR Transnational Code of Conduct Officially Approved After EDPB Opinions 16/2021 and 17/2021**". This first GDPR transnational code of conduct was officially approved after an EDPB Opinion and may serve as model for future codes of conduct. The currently presented EU Data Protection Code of Conduct for Cloud Service Providers is especially relevant as the code applies in an area with massive international data flows. Vander Maelen particular highlights that the recent decisions show that such codes as potentially powerful instruments are (finally) off to a good and will need to prove their potential in the future.

Consistency, however, goes beyond the European Union. *Sebastian Zeitzmann* reports on the recently entered into force "**Council of Europe's Tromsø Convention on Access to Official Documents**" as an important step setting minimum standards in this field. With the report we draw attention to the context of the Council of Europe, which deserves not to be overlooked when one turns to the 'European level', not least because of Convention 108+ which is still to enter into force. Also, the relevance of information access (requests) as a general instrument, but also because of its possible implications for data protection law, when it comes to the protection of personal data in information to which access is requested. With all potential the Convention has to set new standards, *Zeitzmann* points out that it did not only take very long for the Convention to have the necessary amount of signatories to enter into force, but still the largest member States of the Council have not committed which results in a clear limitation of the impact the Convention can have currently.

With regard to the second aspect, which was highlighted at the outset and which, especially in a broader context, also concerns questions of coherence, but in particular questions of competences, we are pleased to have reports in this issue on developments from Germany, the Netherlands, Ireland, Italy, Spain and the Czech Republic. Against this background, however, the case law of the CJEU also deserves special mention, which not only deals with data protection aspects in partial aspects, as in the case of M.I.C.M.,[5] but also more and more with fundamental questions. While the effects of Schrems II are slowly but surely also becoming apparent in supervisory practice[6] — although the Commission updated the standard contractual clauses on 4 July in this light[7] - the CJEU issued a significant decision on 15 June 2021 in Case C-645/19 (Facebook Ireland and others) on the exercise of the powers of national supervisory authorities in cross-border data processing. According to the CJEU, under certain conditions, a national supervisory authority (in this case the Belgian supervisory authority) can take action against data breaches by internationally operating companies (in this case it was Facebook) even if it is not the lead authority for a specific case (which for Facebook would be Ireland). The CJEU is dealing here in particular with the coherence and cooperation mechanism of the GDPR. If one recalls the multi-million fines against Amazon and Google, for example, by the French CNIL,[8] which also deal in detail with the application of the one-stop mechanism, this ruling comes at a very appropriate time. This could shed a

5 In this decision (C-597/19 - M.I.C.M., ECLI:EU:C:2021:492), the CJEU addresses the question, in the margins of a copyright case, of whether IP addresses of users who commit copyright infringements, in particular, can be systematically collected by access providers and handed over to rights holders.

6 See for example the decision of the Portuguese data protection authority of April 27, 2021 (Deliberação/2021/533 available at 875), which stopped the data transfer of the national statistics institute for the census on the basis of Schrems II, or the notification of the German data protection authorities, which point out that the new EU standard contractual clauses have not changed the supplementary obligations under Schrems II (available at <https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/datenschutz-aufsichtsbehoerden-ergaenzende-pruefungen-und-massnahmen-trotz-neuer-eu-standardvertragskla/>)

7 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C/2021/3972, OJ L 199, 7.6.2021, p. 31–61.

8 Cf. on this already the introduction to the reports section of issue (2020) 6(4) EDPL 549 – 553.

new light on such type of decisions taken at national level.

The report of *Julien Levis* and *Philipp Fischer* on "**GDPR 'Glasnost': the Spanish AEPD raises the transparency bar and sanctions two banks**" deals with a decision of a national DPA. The authors not only illustrate some comparisons to a similar decision of the French CNIL as well as the guidance of the former Article 29 Working Party but also highlight the consequence of the approach of the national DPA for the broader context of privacy notices of companies in general. *Levis* and *Fischer* also analyse and question the practicality of the high standards for information obligations set out by the DPA as well as procedural aspects of decision finding. Such a very special approach by judges on national level is also in the focus of the report of *Joost Gerritsen*, who analyses in his report "**Administrative Court Judgment on the Interpretation of Commercial Interests as Legitimate Interests**" how in the Netherlands the court understands commercial interests as not being per se excluded as basis for legitimate processing. Showing how exceptions can be applicable for media based on legitimate interests in light of pursuing commercial purposes, he highlights that the case raises more general questions on the interests of affected – not data processing – third parties vis-à-vis data subjects. In her report "**Supreme Court of Cassation on Automated Decision Making: Invalid Consent if an Algorithm is Not Transparent**" Giorgia Bincoletto deals with the judgement of the Italian Court of Cassation that is of interest well beyond the borders. In this potentially seminal judgment the court issued a clear legal principle according to which the use of algorithms in creating personal profiles which were then made accessible to third persons is only possible if their mode of functioning is transparent. Using algorithms which are intransparent to the data subjects concerned makes their potential "consent" invalid. The further impact of this decision on future decisions by the Italian DPA deserves close observance.

Besides these decisions of courts and DPAs this edition's reports also concern legislative developments.

In her report "**New Act on Privacy and Electronic Communications**", *Kristin Benedikt* introduces us to the new German Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia (TTDSG), which was passed by the German Bundestag on 20 May 2021 (and thereby close to the 25 May which would have made it a special date in light of the applicability date of the GDPR) and primarily updates data protection rules for the online sector in Germany. Partly this law is a (very late[9]) implementation of the 'Cookie Directive' of 2009[10] and partly also anticipates the ePrivacy Regulation currently still debated at EU level. The topic of cookies features very prominently and fits well into the background of the intensive discussions about Maximilian Schrems' NGO NOYB's wide-ranging initiative to fight cookie banners on websites with complaints to data protection authorities across the EU, which may result in a Schrems III (or IV)-decision by the CJEU in the future.[11]

Jan Skrabka's contribution also deals with a legislative development, but in a completely different area. He reports on "**The EU Whistleblowing Directive and its implementation in the Czech Republic: Pandemic and post-pandemic challenges in whistleblower protection**" and does not only address the implementation of rules protecting whistleblowers and thus also investigative journalism from reprisals, which has data protection implications in particular, but also puts this in the context of the impact of the pandemic, which has affected us – and thereby also shaped the Reports Section of the EDPL – a lot lately.

This (still to be observed) importance of Covid-19 for data protection law is underlined in the contribution of *Maria Grazia Porcedda* on "**Data protection implications of data-driven measures adopted in Ireland at the outset of the Covid-19 pandemic**". She analyses the data protection implications of data-driven measures other than tracking apps which otherwise received most attention in media and academic debate. She takes a close look at such measures

9 Cf. on issues in German law regarding the implementation of the ePrivacy Directive Etteldorf, 'Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules', (2018) 4(2) EDPL 235 – 238.

10 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11–36.

11 Cf. on this 'noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints', 31 May 2021, <https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints>.

that were adopted in Ireland to contain Covid-19, puts them into an EU context and also provides suggestions for redressing the measures' shortcomings. In that context she suggests to introduce an overarching instrument containing the blueprint for data processing measures also for future pandemics.

The Reports Section concludes with two contributions in our Practitioners Corner. *Alvaro Moretón* and *Ariadna Jaramillo* deal with the "**Anonymisation and Re-Identification Risk for Voice Data**" analysing several interpretations of the concept of anonymisation provided in the GDPR. The authors focus on the automatic anonymisation of voice data in voice assistants and voice-enabled applications and the issues that may arise from it, particularly the re-identification risk of data subjects and the evaluation of such risk by relying on the H2020 project COMPRISE to further explain the different issues and possible solutions to reach anonymisation of voice data in voice-enabled systems. With this report they supplement an earlier contribution that focussed on how personal data recorded by voice-enabled systems can be identified and what methods can be used to design private-by-design voice-based solutions that intend to neutralise personalisation.[12] Again, this contribution suggests a consistent solution for practical problems that companies in the whole EU are confronted with. *Jens Nebel,* in his report "**Administrative Fines for Infringement of Information Duties: Aggravating and Mitigating Factors in Light of Data Subjects' Indifference**" explores the question of what actual value the extensive information that data processors must provide according to Art. 13 and 14 GDPR has for data subjects in light of these rights being at the heart of the GDPR. To analyse this question, he looks into data from real-life practice inter alia how data subjects interact with information provided as well as the approaches of supervisory authorities to counter the violation of information obligations and then draws concluding lines between these two factors.

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 me at <mark.cole@uni.lu>.

12 Moreton/Jaramillo, 'How can Private Information Recorded by Voice-enabled Systems be Identified?', (2020) 6(3) EDPL 464 – 469.