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.

Introduction

Recent Developments and Overview of the Country and Practitioner's Reports

*Mark D Cole**

Another year is drawing to a close which, once again, has been overshadowed by the impact of the pandemic. Data protection law has played a role in anti-corona measures in many facets - be it in relation to contact tracing, enabling remote teaching at schools and universities as well as working from the 'home office', or the handling of health data in general. While last year the focus in this context was on the shaping of legal measures in line with data protection law, this year many of the approaches taken back then have found their way into decisions of the data protection authorities and courts and thus also into our Reports Section.

The last issue of EDPL this year reflects this development and in particular covers a case from Italy dealing with data protection law issues relating to the facilitation of remote university teaching. *Giorgia Bincoletto* reports on a decision by the Italian data protection authority to fine Bocconi University €200,000 for using software to monitor students taking remote exams. In her contribution '**E-Proctoring During Students' Exams: Emergency Remote Teaching at Stake**' she discusses the different functions that such tools offer (for example, authentication of students via matching biometric data or video surveillance during exams), to what extent this interferes with the rights of students and which violations the Italian data protection authority stated concerning existing data protection law. She also highlights ethical issues in the use of these and similar technologies in such a critical area as education. Since in many places such technologies are not only used in university teaching to keep everyday business (contactless) running even under pandemic restrictions, the complex decision is also relevant across sectors[1] and could impact investigations elsewhere.[2]

In her contribution on '**EDPB Guidelines on restrictions under Article 23 GDPR**', *Christina Etteldorf* deals with questions as to when the rights of data subjects can be restricted by deviating from the provisions of the GDPR by reason of certain public interests and under certain conditions laid down in Article 23. In the now finalised EDPB Guidelines the impact of the pandemic or rather the laws enacted at national level to protect public health and thereby restricting data protection rights of EU citizens are at least an important side note made by the Board even though this aspect was not initially the focus in cre-

DOI: 10.21552/edpl/2021/4/11

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

1 For example, on issues related to the monitoring of workers at the remote workplace, cf eg the Guidelines of CNIL, <https://www.cnil.fr/fr/lecoute-et-lenregistrement-des-appels-sur-le-lieu-de-travail> accessed 9 December 2021.

2 Cf for example the proceedings of the Danish data protection authority against the University of Copenhagen in a similar case, Journal number: 2020-432-0034, <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen>.

ating the Guidelines. However, these Guidelines are just one of many interesting and relevant work results of the EDPB in the past quarter. In addition to a series of opinions on draft decisions of national data protection authorities,[3] the EDPB also published guidelines on the interplay of Art. 3 with international data transfers.[4] Those guidelines are intended to help controllers and processors in the EU in the future to determine whether a processing constitutes an international data transfer and thus triggers special obligations. Especially since the ruling of the CJEU of 16 July 2020 on the EU-US Privacy Shield in the Schrems II case (C-311/18)[5], creating legal clarity in this area has become a pressing issue. Regarding the status of numerous questions arising in the context of data transfers to the US, the EDPB has also commented separately in its response to an inquiry of the United Nations Under-Secretary-General for Legal Affairs and United Nations Legal Counsel on a very specific aspect:[6] The Boards' Chair *Andrea Jelinek* stated that the EDPB will 'take the utmost account of [the] suggestion that the EDPB should consider addressing the situation of all transfers to United Nations System Organisations in a specific set of guidelines'.

However, the interaction with data protection law outside the EU does not only play a role with regard to the US, but also for neighbours that are much closer to the EU. This refers in particular to the United Kingdom, which after its separation from the EU could, at least in principle, pursue different approaches for its territory in the future than those provided for in the GDPR. From an international perspective, the very recent ruling at the end of November by the UK Supreme Court in the case of Lloyd vs. Google, on which *Matt Getz* and *Kimmie Fearnside* report in this issue, was therefore eagerly awaited,. In their contribution '**Lloyd v Google: U.K. Supreme Court on represented actions for personal data breach claims**' the authors discuss the SC's decision, which was mainly about what is known as Google's "Safari Workaround" with which privacy settings concerning third party cookies on iPhones could be circumvented when the users where surfing the Internet via the Safari browser. The case is therefore about the violation of Apple users' rights in substance. However, the very interesting aspect here is that the Court also had the opportunity to weigh in on whether England's long-standing procedure of representative actions could be used in a comparable way to US-style class actions to bring mass claims for breaches of data protection legislation. *Getz* and *Fearnside* discuss why the answer was negative in this specific case, what this means for the collective pursuit of data protection rights and which impact the decision has in view of data protection law in the EU. This latter aspect concerns particularly the question of whether the award of compensation also requires, in addition to an infringement of data protection law as such, that an applicant must have suffered harm. With regard to Art. 82 GDPR, the CJEU will soon have to take a position on this on the basis of a referral decision from Austria.[7] But other proceedings before the CJEU also require answers to developments similar to those presented in Lloyd v. Google. On 2 December 2021, in his Opinion in Case C-319/20 - Facebook Ireland, Advocate General *Jean Richard de la Tour* argued in favour of the possibility that consumer protection associations can bring representative actions for infringement of EU privacy rules against data processors such as Facebook, before national courts.[8]

In relation to the above-mentioned Facebook case and the use of personal data, there is another very relevant topic for business practice that is addressed in this issue: targeted online advertising. The conversation has shifted from 'cookies' to the alternatives that the ad tech sector will/could use in the future or is already relying on. The French CNIL recently issued a comprehensive communication – very

3 Cf for an overview <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en>.

4 Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_de> accessed 9 December 2021.

5 Cf on this Virgílio Emanuel Lobato Cervantes, 'The Schrems II Judgment of the Court of Justice Invalidates the EU – U.S. Privacy Shield and Requires 'Case by Case' Assessment on the application of Standard Contractual Clauses (SCCs)' (2020) 6 EDPL 4, 602-606.

6 EDPB response to Mr Miguel de Serpa Soares regarding the ongoing dialogue between the EDPB and the United Nations on data protection (23 November 2021), <https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mr-miguel-de-serpa-soares-regarding-ongoing_de> accessed 9 December 2021.

7 Case C-300/21, Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021, *UI v Österreichische Post AG*.

8 Opinion of Advocate General Richard de la Tour delivered on 2 December 2021 in Case C-319/20, *Facebook Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*

recommendable for an overview read – on alternatives to first-party cookies and the consequences that arise in terms of data protection law when they are implemented.[9] This also includes so-called fingerprinting – a technique that creates a unique fingerprint by combining device-related information sent for example by the browser when surfing the internet, thus enabling the tracking of users. This technique, which is commonly said to be even more intrusive than cookies, is the subject of *Paarth Naithani's* contribution in the Practitioner's corner - '**Regulating the 'Fingerprinting Monster' Through EU Data Protection Law**'. This report looks at the possibility of regulating such fingerprinting under the existing and future data protection framework in the EU by investigating the question of whether fingerprints constitute personal data and if their processing requires users' consent or can rely on a legitimate interest basis. In addition to the data protection and ePrivacy legal framework as set by the GDPR and ePrivacy Directive or the proposed ePrivacy Regulation, this also includes issues in the context of the use of artificial intelligence, which are taken up in the Commission's proposal for an AI Act[10]. The author raises awareness of the 'fingerprinting monster' that users are already facing – and might not even know about.

The AI Act is not the only legislative development that plays a role in the Reports section of this issue[11] as *Corina Kruesz* and *Felix Zopf* report on another 'Act'. Currently a lot of focus in Europe is on the Act-'Twins' Digital Services Act and the Digital Markets Act, on which the Council founded its General Approach[12] at the end of November and which are also highly relevant from a data protection perspective. But the authors in this report discuss the proposed Data Governance Act (DGA), which has been less in the limelight so far and is therefore given its rightful place here. As regular readers will spot, we are doing so in a longer than usual contribution in order to give you an extensive overview of the of the original proposal of the Commission for the DGA as well as first statements in the legislative process and input from the EDPB and EDPS DGA, the report being titled '**The Concept of Data Altruism of the draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU'**. The authors put the Commissions' approach to increase trust in data sharing or, more precisely, in data altruism organisations, as well as at improving the means and tools to manage consent-based personal data sharing for the common good at large scale in context especially with the GDPR and the Regulation on the free flow of non-personal data. They suggest implementing a regulatory sandbox model next to the proposed rules on data altruism which would likely incentivise both individuals giving (personal) data as well as data altruism organisations. This recommendation remains relevant and the DGA likely will soon be enacted after the trilogue negotiations reached a compromise after completion of this edition's report.[13]

Another important new Directive proposal is addressed by *Sandra Schmitz-Berndt* in her contribution '**Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way**'. This contribution comes in midst of an ongoing legislative process and provides valuable insights into developments related to security of network and information systems and their impact on data security and protection. After the first piece of EU-wide cybersecurity legislation, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, had to be transposed into national law by May 2018. A reform of the Directive is already on its way. *Schmitz-Berndt* highlights how the proposed 'NIS 2.0' addresses shortcomings identified in the current version of the NIS Directive and comments on the most recent amendments suggested by the European Parliament's Committee on Industry, Research and Energy (ITRE). Considering the speed of the initial review of the NIS 1.0 and the challenges posed by the COVID-19 crisis, she

9 CNIL, 'Alternatives to third-party cookies: what consequences regarding consent?', (23 November 2021), <https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent> accessed 9 December 2021.

10 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final.

11 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.

12 General approach on the DSA, ST 13203 2021 INIT, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_13203_2021_INIT> accessed 9 December 2021; General approach on the DMA, ST 13801 2021 INIT, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_13801_2021_INIT> accessed 9 December 2021.

13 Cf press release European Commission of 30.11.2021, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6428> accessed 9 December 2021.

points out that it is unlikely that the time it takes to adopt a NIS 2.0 will be as long as the three years it took to adopt the original NIS.

This issue of EDPL 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. As usual, we would like to extend our thanks to *Christina Etteldorf*, Research Associate at the EMR, who puts together EDPL's reports section and manages the reviews together with me. Without her input we would not be able to provide such a broad overview of topics. We invite you to continue to suggest reports on future national and European developments to us to make sure we can cover as many relevant aspects of data protection law developments as possible. To submit a report or to share a comment please reach out to me at <mark.cole@uni.lu>. Finally, we would like to wish all our readers a safe and healthy end of year and an equally safe and happy new year 2022 which will certainly continue to bring relevant developments in privacy law but hopefully will also allow us to leave our private surroundings again more easily so we can discuss and debate with each other 'in real'!