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**

Five years is a first small jubilee, but as the General Data Protection Regulation has become such a permanent companion in data protection developments, its upcoming 5th birthday since it became applicable in May 2018 might go unnoticed. This may also be a result of the daily application of the GDPR rules by the supervisory authorities in the Member States of the EU as well as by decision-making of the European Data Protection Board (EDPB), both of which we will be reporting about in this edition's Reports Section. In addition, the GDPR is not alone and will likely have further companions on the EU level soon. The legislative initiative of the European Commission for a Data Act is progressing: on 14 March 2023 the European Parliament adopted its position[1] on the proposed regulation with 500 votes in favour, 23 against and 110 abstentions. Before the trilogue negotiations can commence, the Council's General Approach has to be awaited, a process which seems to be dragging on.

A topic that has been simmering ever since the GDPR came into force seems to have taken on particular relevance in the discussion in recent months, namely the collection and further processing of personal data by credit agencies. Such private companies or other entities exist in most Member States –although there are of course national differences in the setup and methodological approach. Their activity essentially consists of collecting data on the economic capacity of consumers and, based on this, assigning them a score – therefore referred to as credit scoring – which is supposed to be an objective value that provides information on their creditworthiness, for example, to companies that want to make business with these consumers and calculate their risk of not receiving payments eventually. The procedures and parameters used for this credit scoring are often not transparent and there is typically automation to a differing degree involved. This makes the credit agencies correspondingly less popular with consumers, because their score is decisive whether they can get a loan from a bank or rent a place to live, for example, even though they can rarely successfully defend themselves against the score if they think the result is incorrect. As the data used for the scoring obviously is closely connected to the individuals and their behaviour and therefore personal data as protected by the GDPR, the interpretation of data protection law in this regard has the potential of significantly influencing the future practice in this sector. On 16 March 2023, the Court of Justice of the European Union's Advocate General Priit Pikamäe issued

DOI: 10.21552/edpl/2023/1/9

* 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 Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), P9_TA(2023)0069, <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.html> accessed 2 May 2023.

two opinions on data protection aspects in connection with the activities of credit agencies – in both cases with regard to the German SCHUFA[2], but likely with relevance for other similar institutions. In both cases, the opinion is probably regarded as unsatisfactory by credit agencies.

In the joined cases C-26/22 and C-64/22[3], the main issue concerned the periods until the collected data is deleted. Following the rules as laid down in German insolvency law, two consumers had received a discharge of residual debt after their insolvency and this information had been made publicly available by the competent authorities and deleted after 6 months. However, SCHUFA had collected this information about the consumers and – on the basis of codes of conduct agreed with the data protection authority in charge – provided for a storage period of that data for three years. Loans were refused to the individuals concerned on the basis of their negative score and requests for deletion of that data were unsuccessful. In a preliminary reference procedure, the Advocate General comes to the main conclusions that (1) Art. 6(1) (f) GDPR precludes the storage of data from public registers (Art. 79(4) and (5) GDPR) beyond the storage period of the register foreseen by law (other possible justifications for a prolonged retention period would have to be examined by the referring national court), (2) data subjects have a right to erasure under the GDPR in these cases, and (3) codes of conduct, even if approved by a competent authority under Art. 40(2) and (5) GDPR, cannot establish legally binding derogations from Art. 6(1) GDPR. Case C-634[4] concerns the determination of the score value and the question of whether this constitutes an (unlawful) automated decision-making under Art. 22(1) GDPR. The Advocate General affirmed that this was already the case with regard to the automated creation of a probability value about the ability of a data subject to service a loan in the future. This is the case if this value is transmitted to a third party and this third party (e.g. banks, landlords, employers, etc.) bases its decision about the establishment, implementation or termination of a contractual relationship with the data subject to a relevant extent on this value according to established practice. The Advocate General emphasises that there may be cases in which, despite a negative score value, the human decision of the third party is decisive (which again needs to be examined by the referring national court) and thus there would not be a violation of Art. 22(1) GDPR. However, in light of the fundamental rights to protection of personal data and privacy, the most protective way for the rights holders was to hold the credit agencies responsible because of the initial creation of the score value and not to focus on the subsequent use of this score by economic entities. In the reaction to the opinion, the SCHUFA appeared relaxed.[5] Apart from the fact that the opinion is not binding (the final decision has to be taken by the judges of the CJEU), the Advocate General did not give an opinion on the legality of the specific method of calculating the score value itself.

In Austria, the data protection NGO noyb also achieved success in its action against the credit agency CRIF (which is active in several countries). Core data (name, address, date of birth, gender) of Austrian citizens that CRIF uses to calculate score values came to a large extent from the address publisher AZ Direkt. However, the address publisher would only have been allowed to pass on this data for marketing purposes and not for purposes of determining economic capability of individuals, which makes the data transfer unlawful and necessitates its deletion according to the decision of the Austrian data protection authority of 18 March 2023.[6] Just two weeks earlier, on 2 February2023, the Austrian data protection authority had also ruled – in response to yet another case brought by noyb – that the data collection and storing behaviour of the largest credit agency in Austria, Kreditschutzverband von 1870 GmbH (KSV), was illegal. It had created entries in its database and queried further data in registers on the occasion of GDPR requests for information from data subjects (even despite precautionary objections of the requesting data subjects). This retrieval of civil registry data by credit agencies and the subsequent storage of the data in a 'business database' violates

2 The SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) is the leading German provider of such services and according to their own information holds data on 6 million companies and 68 million private persons and supplies answers to 300 000 information requests daily on average; cf. --<https://www.schufa.de/ueber-uns/schufa/so-funktioniert-schufa/> accessed 2 May 2023.

3 ECLI:EU:C:2023:222 - UF (C-26/22) and AB (C-64/22) / Land Hessen.

4 ECLI:EU:C:2023:220 – OQ / Land Hessen.

5 Cf. press release of 17.3.2023, <https://www.schufa.de/themenportal/schufa-aeussert-eugh-verfahren/> accessed 2 May 2023.

6 Cf. On this the press release of noyb (27.3.2023) with further reference to the decisions, <https://noyb.eu/en/majority-credit-bureau-crif-database-illegal?mtc=mu> accessed 2 May 2023.

the right to confidentiality because the underlying data processing is unlawful.[7]

Besides the role of the national supervisory authorities in these developments, the EDPB is continuing to underline its institutional relevance in enforcing GDPR rights. This important role can be seen in its contribution to evaluating the most recent attempt to find a way of allowing in a simple but legally certain way the transfer of personal data by companies from the EU to the U.S. The political agreement between the two sides on a new 'EU-U.S. Data Privacy Framework' is the basis for the planned adequacy decision by the European Commission, which in its draft state necessitates a commenting opinion by the Board. *Sandra Schmitz-Berndt* reports on this opinion in her report '**EDPB Opinion on the European Commission's Draft Adequacy Decision regarding the EU-U.S. Data Privacy Framework: Is the Scene Set for Schrems III?**'. She discusses the criticism made by the EDPB despite a general acceptance of this new framework which is regarded by the supervisory authorities convened in the Board as a major step forward compared to the previous setups which had been annulled by the CJEU – but she also ask the question whether there will be a new decision by the CJEU in light of the continued criticism, whether this were to be brought to the courts by Maximilian Schrems and noyb or any other data protection NGO or individual concerned.

The EDPB is not only involved in opinions in connection with legislative proposals on EU level but mainly – and as is well known to our regular readers as we frequently cover this part of EDPB's activity in the reports section – as the forum for exchange between the national supervisory authorities of the EU Member States in matters of cross-border relevance. This competence includes a kind of dispute resolution function in which the Board can take decisions if other DPAs are not satisfied with the action that a lead supervisory authority is intending to take and does not react to the wishes and requests in a way that satisfies the complaining authorities. The mechanisms foreseen in Art. 65 GDPR have involved mainly controversies between the Irish Data Protection Commission (DPC) as lead supervisory authority and many of the other DPAs and based on a differing assessment of the way data protection violations by companies with a seat in Ireland should be reacted to. Meta was subject of three decisions of the EDPB which influenced the final decision of the DPC concerning data processing in its WhatsApp, Facebook and Instagram services. *Maria Magierska* gives a detailed overview in her report entitled '**Three EDPB binding decisions in the Art. 65 GDPR procedure and two major questions for the future**' in which she also shows which lessons should be learnt for future cases and potential amendments of the (procedural) framework in protecting individuals GDPR rights more effectively. Following up on the EDPBs Binding Decisions as well as the final decisions of the DPC as presented in the report, Meta announced[8] to update its privacy practices regarding personalised advertising. From 5 April 2023 Meta intended to change the legal basis that it uses to justify advertising based on the massive amounts of personal data gathered from contractual necessity (Art 6(1)(b) GDPR) to legitimate Interests (Art. 6(1)(f) GDPR) for the processing concerning Union citizens. However, this 'legal change does not prevent personalised advertising on [Metas] platform[s], nor does it affect how advertisers, businesses or users experience [Metas] products', the company 'reassured' their users. Therefore, one can argue that this supposed change in legal basis will not change anything about the potential illegality of the data processing by Meta and could likely lead to a new procedure[9] which will again give the company more time until a further final decision is made and thus allow for a profitable use of the collected data until then. It should be noted, however, that Meta announced that it would give users 'additional options' concerning how 'certain information' is processed to serve behavioural advertisements.

The only report dedicated to a decision in only one State in this edition's Reports Section is actually of equal importance across Europe and during the time of drafting the report already a new taskforce has been created within the EDPB[10] taking care of the matter. We are referring to the topic that everyone

7 GZ: D124.3614/22, <https://noyb.eu/sites/default/files/2023-02/DSB_KSV1870_Redacted.pdf> accessed 2 May 2023.

8 Meta, 'How Meta Uses Legal Bases for Processing Ads in the EU', Update of 30. March 2023, <https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/>.

9 Noyb has already announced taking action, see press release of 30.3.2023, 'Meta (Facebook, Instagram) switching to "Legitimate Interest" for ads', <https://noyb.eu/en/meta-facebook-instagram-switching-legitimate-interest-ads> accessed 2 May 2023.

10 EDPB, ‚EDPB resolves dispute on transfers by Meta and creazes task force on Chat GPT' (13 April 2023), <https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_de> accessed 2 May 2023.

seems to be talking about these days: the way that ChatGPT catapulted 'artificial intelligence' into the centre of attention in the media and on the streets. And we are not just mentioning it, to follow the trend, but because there is a remarkable development. While there are intensive political and societal debates across the world[11] whether and how one should consider regulating AI or applications such as ChatGPT, a first decision with direct consequences for the company and the offering of the (free) software application on the market has been taken. And it was taken by a supervisory authority in charge of data protection. The Italian DPA banned in a much-discussed urgency procedure temporarily the offer of ChatGPT to users in Italy until corrective measures on the side of OpenAI, the operating company, have been implemented. We are very happy that we can provide already in this edition a very timely overview of the decision and an overview of parallel activities that have resulted in the days after the Italian decision became publicly known. *Pier Giorgio Chiara* covers the controversy in his report, '**Italian DPA v. OpenAI's ChatGPT: The Reasons Behind the Investigation and the Temporary Limitation to Processing**'.

Finally, in our Practitioners Corner we cover yet another use of automated tools that have potentially very negative outcomes for individuals and can lead to discrimination, just like the aforementioned credit score systems and ChatGPT. In her piece, *Florence D'Ath* gives a detailed overview of tools used in connection with employment decisions and their potential legal problems. Her report '**EU Data Protection Law as a Tool against Discriminatory Outcomes in the context of E-recruitment**' shows how the rules of the GDPR can actually help in protecting rights of individuals beyond the mere protection of their personal data, in this case by giving them a tool against discriminatory effects of automated tools in recruitment practices.

This overview of our reports hopefully demonstrates not only the relevance of the topics covered, but also their timeliness – both of which we can provide thanks to our experts. We, the Editors together with the Institute of European Media Law (EMR), hope to meet your interest with these reports and are looking forward to receiving suggestions for reports on national and European developments in the future that you would like to see in this section: 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>.

11 The U.S. government has opened a policy request for comment on AI accountability in order to obtain views on how to regulate AI applications in future, see National Telecommunications and Information Administration, 'AI Accountability Policy Request for Comment' (13 April 2023) <https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment> accessed 2 May 2023. The Chinese government already went a step further: On 11 April 2023 the Cyberspace Administration of China (CAC) - the national internet regulator of the People's Republic of China - released draft Administrative Measures for Generative Artificial Intelligence (available in Chinese at <http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm>) which are open for public consultation until 10 May 2023. According to the draft, inter alia, Chinese tech companies would need to register generative AI products with the CAC and submit them to a security assessment before they can be released.