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*

In data protection terms, the past few months were dominated by news around proceedings in reaction to data protection violations by various social networks.

TikTok, which is still sharply rising in popularity in Europe and is operated by the Chinese company ByteDance, announced in July 2022 that it intends to change its terms of service. While the social network had recently shown its goodwill in terms of compliance with the EU legal framework concerning consumer protection and advertising,1 alarm bells have been ringing in terms of data protection law as the announcement included the plan that targeted advertising would no longer be carried out based on consent, but on the grounds of legitimate interests. This ‘creeping’ change of significant conditions that users would have had to accept if they wanted to continue using the service is inevitably reminiscent of the announcement of the change of WhatsApp’s terms of service in May 2021 with which users would have automatically agreed to a merging of their data in the Meta Group. At that time, this not only alerted (for Meta non-leading) data protection authorities in the EU, but also was a crucial factor in the proceedings before the EDPB and ultimately in the final fine imposed by the Irish (lead) supervisory authority (the Data Protection Commission, DPC).2

Now, just over a year later, we can once again observe quick reactions of non-lead supervisory authorities. After clear warnings from inter alia the Italian3 and Spanish4 supervisory authorities, TikTok decided to ‘pause’ its plans.5 However, this does not apply to other behaviour that is considered critical under data protection law and for which TikTok has been under scrutiny of EU data protection authorities for a long time, namely the (unlawful) processing of personal data of minors and data transfers to China, for which the EDPB has even set up a dedicated investigative task force.6 For the specific aspect of the protection of minors’ data, the Irish DPC has most recently in September submitted its Article 60 GDPR draft decision to other concerned supervisory authorities in the EU.7 The Inquiry focuses on basic settings

DOI: 10.21552/edpl/2022/3/8

* 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>.


2 Lisette Masten ‘The EDPB’s second Article 65 Decision – Is the Board Stepping up its Game?’ (2021) 7(3) EDPL 416-422.


4 AEPD (12 July 2022), <https://twitter.com/AEPD_es/status/1546818248301330432/ref_src=twsrc%5Etfw>.


6 Cf. on this in detail Christina Etteldorf, ‘The Clock is ticking for TikTok – How to protect underage EU citizens?’, DPOblog (6 November 2021), <https://dpojournal.eu/the-clock-is-ticking-for-tiktok-how-to-protect-underage-eu-citizens>.

of the TikTok platform, in particular the setting that 
puts processing public-by-default in relation to 
accounts of users under the age of 18 as well as age 
verification measures for persons under 13. In addition, 
the compliance with transparency obligations vis-à-
vis this vulnerable category of users is one of the 
main topics of the draft decision.

In another procedure involving the cooperation 
mechanism in cross-border matters and concerning 
the question of data transfers there is important 
news: the DPC has sent its draft decision on the Face-
book/Meta case to its colleagues in Europe. Accor-
ding to media reports, the authority wants to block 
the transfer of data from Meta to the United States 
of America. However, there is no mention of a penalty 
for the consequently illegal data transfer of the past 
years. While these proceedings will still go through 
the cross-border mechanism of the GDPR, the case 
against Instagram has finally reached an outcome. 
Following the EDPB’s binding decision in late July, 
the DPC in mid-September has announced a fine of 
€405 million and a range of corrective measures. 
The decision concerns, in particular, the public disclo-
sure of email addresses and/or phone numbers of 
children using the Instagram business account fea-
ture and a public-by-default setting for personal Inst-
agram accounts of children.

However, the ‘social media giants’ do not only have 
to fear severe sanctions by data protection authori-
ties, but also might run into trouble in other context. 
This is documented by the opinion of the Court of 
Justice of the EU’s Advocate General Rantos which 
he delivered on 20 September 2022 in the case of Meta Platforms. In essence, this case is about the 
decision of the German Federal Cartel Office prohib-
iting Meta Platforms from processing data as pro-
vided for in Facebook’s terms of service and from im-
plementing those terms, relying on the reasoning 
that this (unlawful) processing constitutes an abuse 
of the company’s dominant position in the social 
media market for private users in Germany. Questions 
arising in this context on the relationship between 
competition law and data protection law as well as 
on intersectoral (data protection authorities or com-
petition authorities) and territorial jurisdiction (Ger-
many or Ireland) are answered by the AG in the sense 
that, yes, a competition authority, within the frame-
work of its powers under the competition rules, may 
examine, as an incidental question, the compliance 
of the practices under investigation with the GDPR 
rules. However, it then has to take into account any 
decision or investigation of the competent (lead) su-
ervisory authority in the framework of the GDPR, 
informing and, where appropriate, consulting the na-
tional supervisory authority. The AG bases this oblig-
ation on the duty to cooperate in good faith enshrined 
in Article 4(3) TEU due to a lack of cross-sectoral co-
operation rules. In conclusion, the AG’s opinion 
means that if the Irish DPC had already assessed the 
processing activity of Meta subject to the proceed-
ings as lawful, the German Federal Cartel Office in 
principle would not have been allowed to base its 
competition law decision on unlawful processing to 
justify an abuse of market power. The CJEU’s ruling 
in this case will be eagerly awaited, especially in view 
of its interconnections with the newly agreed regu-
lation, the Digital Markets Act.

Less of a surprise or novelty were the rulings on 
French and German data retention, in which the 
CJEU once again assessed variants of obligations (cre-
ated by national law) to retain traffic and location da-
ta by providers of electronic communication services 
without specific reasons. These were – unsurprising-
ly – declared to be in breach of the ePrivacy Direc-
tive, as has been the case with data retention schemes 
of the Member States previously.

Another ruling, or rather a referral to the CJEU in 
a different matter, which concerns the interpretation 
of the notion of legitimate interests in a commercial 
environment and which many in the data protection 
community, especially in the Netherlands, had hoped 
for, will have to wait a while longer for its final out-
come. The Dutch State Council has delivered its long-
awaited decision in ‘Voetbal TV’ which concerns a 
penalty (€575,000) imposed by the Dutch DPA on the 
video platform Voetbal TV due to recording amateur 
football matches on behalf of football clubs and mak-
ing them available online without consent of the
(mostly underage) players. 12 Beyond this specific fine, however, this case is about the Dutch DPA’s interpretation that data processing for purely commercial purposes cannot, in general, be justified relying on legitimate interests, which the authority has also pointed out in a standard declaration. 13 This standard declaration had alerted the European Commission 2020, which in a letter to the Dutch DPA – only recently uncovered in the context of a request for information by the Dutch newspaper NRC – expressed its ‘concern’ about a (too) strict interpretation of the GDPR in its view. 14 The Commission stated that it was not compatible with the case law of the CJEU, recitals 4 and 47 of the GDPR and the different interpretations by the Article 29 Working Party and therefore very clearly requested the Dutch DPA to amend the wording of its standard declaration to make clear that commercial interests can be considered as ‘legitimate’ interests if they are not overridden by fundamental rights and freedoms of the data subject which always needs to be checked in a specific balancing exercise. However, the Dutch DPA did not change its supervisory practice in response to this; rather, a number of further proceedings based on the strict interpretation are pending before the domestic courts. This will not change with the decision of the State Council, because although it indeed overturned the specific decision of the DPA, it based this on the fact that the DPA had already erroneously carried out the first step of the three-step examination required under Art. 6 para. 1 lit. f) without taking into account all functions of the platform (eg. game analysis, exchange of players, players who want to be presented, etc.) in its examination, ie. by already incorrectly identifying the interest as being purely of a commercial nature. Therefore, in the opinion of the State Council, comments on the second and third steps of the test (necessity and weighing of interests) were no longer necessary in the present case and thus it also rejected the need for a referral to the CJEU, which had been requested in the proceedings.

In contrast, another significant matter from the point of view of companies operating online, with a European-wide significance for the marketing industry, will have to be decided by the CJEU due to a pending referral. The Court of Appeal Antwerp forwarded the decision of the Belgian supervisory authority on the Transparency and Consent Framework of IAB Europe, 15 to the CJEU and asked in the preliminary reference in particular whether the consent string alone or in combination with the IP address constitutes personal data and whether IAB Europe can be qualified as a (joint) controller in collecting this. 16 The EDPB has continued its high pace of activity in the previous months, publishing inter alia another Art. 65 binding decision concerning Accor SA, a statement on the European Police Cooperation Code, 17, an EDPB-EDPS Joint Opinion on the child sexual abuse regulation proposal 18 and an opinion on certification criteria. 19 Noteworthy is the open letter on the EDPB budget proposal for 2023 in which the Board expresses its deep concerns that the 2023 budget, if not substantially increased, will be far too small to allow the EDPB and the EDPS to fulfil their tasks appropriately. 20 Receiving continued new tasks from the legislator, the EDPB ‘strongly urges support’ for its budget request which includes eight additional staff members each for the EDPB and EDPS Secretariat. This would still be a small contribution in view of the pillars that the EDPB wants to support with such additional staff: credibility of enforcement (as national DPAs are intensifying their enforcement activities leading to more disputes requiring the EDPB’s inter-

---

15 Cf. Kristin Benedict ’Belgian Data Protection Authority Ruling - Online Advertising on the Brink of Extinction?’ (2022) 8(1) EDPL 85-89.
vention), robustness of enforcement (higher fines lead to more litigation requiring robust and well-reasoned decisions) and predictability of the legal framework.

In the Reports Section of this edition of EDPL two other published texts of the EDPB are taken up.

Carl Vander Maelen deals with the EDPB’s new guidelines on codes of conduct for international data transfers in his contribution ‘EDPB Releases Final Version of ‘Guidelines 04/2021 on Codes of Conduct as Tools for Transfers’ – An Important Step with some Rough Edges’. He examines the formal and substantive requirements set by the EDPB for the development of such codes of conduct, the role of the supervisory bodies in this process and the significance of these codes for practitioners, who are thus provided with another means for ensuring compliance with an adequate level of data protection when transferring data outside the EU. Besides some potential for clarifications and improvement, the author assesses Guidelines 04/2021 in their final version as an important step for more legal certainty.

Giorgia Bincoletto reports on the EDPB-EDPS Joint Opinion on the Commission Proposal for a Regulation on the European Health Data Space published in July. Based on a summary of the main rules of the Commission’s proposal of May 2022, which includes not only provisions on the use of electronic health data and the development of corresponding systems and applications, but also on monitoring by a new European Health Data Space Board, she addresses the remarks and also criticisms that the EDPB and EDPS raise regarding the proposal. Her contribution ‘The EDPB-EDPS Joint Opinion on the Commission Proposal for a Regulation on the European Health Data Space: key issues to be considered in the legislative process’ highlights in particular the need for cross-border sharing, access, and further use of these categories of data both for the provision of healthcare and for other following purposes and public interests. However, given the highly sensitive nature of personal health data, the risks of unlawful access to it should be carefully addressed in the Regulation, which will therefore be the task for the legislative bodies in the upcoming process. This is especially true in light of the fact that the EHDS could serve as a blueprint for the future regulation of other sectors such as the others that were announced in the Commission’s data strategy.21

Picking up on the topics described in our introductory remark, Marcelo Corrales Compagnucci reports on a case from Denmark also evolving around protection of minors and transatlantic data transfers but in a completely different scenario. As the title ‘Danish DPA Banned the Use of Google Chromebooks and Google Workspace in Schools in Helsingør Municipality’ already suggests, the contribution discusses the proceedings of the Danish DPA on the implementation of certain Google applications used in classrooms of Danish primary schools and their (un)lawfulness. Despite some safeguards put in place, the inclusion of EMEA cloud services and restrictions in Google Chromebooks and Workspace applications, the authority has found the use of that hardware and software to be incompatible with the requirements of the GDPR, especially because of the lack of adequate safeguards for data transfers to the US and the special protection for underage students. The author not only shows the details of the decision, but also its background in the Schrems II case and the status of currently available options to solve this problem for Danish municipalities.

Also highly topical against the background of the aforementioned news from the CJEU, Adrien Battacci takes up the issue of data retention regimes and reports on recent developments in Portugal. His contribution ‘Judgment n.° 268/2022 of the Portuguese Constitutional and its Contribution to the European Dialogue on Metadata Retention and Access Regimes’ analyses the decision of the Constitutional Court in light of the Portuguese regime of metadata retention, which integrates the standards set by the CJEU but also extends them by applying the right to informational self-determination to legal persons and by further developing its concept of communicational self-determination. This in particular alludes to the rights of data subjects in the digital environment.

Gaurav Pathak deals in his report ‘Manifestly Made Public: Clearview and GDPR’ in the Practitioner’s Corner with the latest developments around the facial recognition software Clearview AI and its compliance with data protection law which was questioned by several data protection authorities in Eu-

ropes and beyond in the recent past. The author gives a brief overview of decisions from Australia, Canada, France, Italy, Greece and the UK and reflects the main points of criticism under data protection law, thereby showing the high practical relevance of limits to such facial recognition databases and their use. This essentially revolves around the question to what extent it is relevant in terms of data protection law that the data Clearview AI uses (the software scrapes the internet for photos of people, saves them in a database and allows customers [mainly police authorities] to search with and for images and, in the end, people) were freely accessible on the open internet anyway and the search results therefore only refer to freely accessible sources as well. This question and its answer by authorities also has considerable relevance for millions of data subjects and will certainly be subject for further litigation.22

Finally, we are pleased to once again have a piece dealing with developments in data protection law in the Council of Europe. Rowin Jansen and Minke Rei
jneveld report on ‘Convention 108+, the GDPR, and Data Processing in the National Security Domain’ and analysing how the legal order of the Council of Europe is more and more influencing national activities in the security sector. The authors in particular highlight areas in which Convention 108+ can have an impact also on the EU legal order by pointing to differences in the scope of application between the GDPR (which in principle excludes the national security and intelligence domain) and Convention 108+ (explicitly including the national security domain). The report demonstrates the legal consequence this might have, especially with regard to oversight mechanisms, and concludes that it is not unlikely that Member States might have to strengthen the legal safeguards for the privacy protection of citizens in this context.

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>.