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 our last issue, we featured a report on the rather critical opinion of the European Data Protection Board (EDPB) concerning the Commissions' draft adequacy decision[1] regarding EU-US data transfers.[2] Only a few weeks later, the European Parliament concluded in its resolution of 11 May 2023[3] 'that the EU-US Data Privacy Framework fails to create essential equivalence in the level of protection' and therefore called on the Commission not to adopt its draft decision but rather to continue negotiations with its US counterparts. The Parliament members stated in clear terms what lead them to this conclusion by pointing out that the Data Privacy Framework principles issued by the US Department of Commerce had not been sufficiently amended in comparison to those that had existed under the Privacy Shield which was invalidated.

In particular, the US Intelligence Community would have time until October 2023 to update its policies and practices in line with the commitment of the EO 14086; further, the US Advocate General had yet to name the EU and its Member States as qualifying countries to be eligible to access the remedy avenue available under the Data Protection Review Court foreseen. Therefore the Commission was 'not in position to assess the effectiveness of the proposed remedies and proposed measures on access to data 'in practice'', thus, can 'only proceed with the next step of an adequacy decision once these deadlines and milestones have first been completed by the US'.

However, before the expiry of the relevant deadlines and apparently seeing no need for further negotiations, the Commission adopted its adequacy decision[4] on 10 July 2023.[5] Contrary to the widely voiced concerns from the perspective of data protection, a legal framework has now - once again - been created that provides (for the moment)[6] the basis for GDPR-

DOI: 10.21552/edpl/2023/2/10

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

1 Draft Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (13.12.2022), <https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en> accessed 1 July 2023.

2 Sandra Schmitz-Berndt, '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?' (2023) 9(1) EDPL 61-67.

3 European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework, P9_TA(2023)0204.

4 Commission Implementing Decision of 17.6.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final, <https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf> accessed 1 July 2023.

5 European Commission 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows' (10.7.2023), <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721> accessed 1 July 2023.

6 Maximilian Schrems and its organisation noyb have already announced, although being 'sick and tired of this legal ping-pong' to challenge the new framework before the CJEU. See noyb, 'European Commission gives EU-US data transfers third round at CJEU' (10 July 2023), <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> accessed 1 July 2023., paving the way for a Schrems III (or IV, with regard to pending case Case C-446/21) decision.

compliant data transfers to the US.[7] In addition to the goal to 'deepen [the] economic ties between the EU and the US'[8], aspects of creating legal certainty for EU data controllers were likely on the 'pro' side of the Commission's 'balancing exercise'. Applications and tools from US companies, which are part of the standard portfolio in everyday business and especially in the online economy, had to be treated with the utmost caution since the fall of the Privacy Shield[9] if they were linked to data processing on US servers.[10] Especially in recent months, injunctions by courts and data protection authorities have become more frequent.

For example, the Federal Administrative Court of Austria has declared the implementation of Google Analytics on a website to be non-compliant with Art. 44 GDPR,[11] thus ultimately confirming a decision of the Austrian data protection authority which we had covered in an earlier report[12], and that many supervisory authorities in other Member States[13] had also taken in a similar manner. A business-friendly interpretation in the sense of protecting the free movement of data - an objective that the GDPR also pursues in addition to the protection of privacy - was out of the question for the court: economic interests had also not played a role in the Schrems II ruling of the CJEU, the Austrian judges argued.

While these decisions are directed at the (EU) users of the tools, e.g. website or app operators, who regularly can do little or even nothing to establish an adequate level of data protection as required by the GDPR except refraining from using the tools altogether, another significant decision was directly addressed to one of the US tech 'Big Five', thus addressing the root of the problem. We are referring to the recent decision of the Irish Data Protection Commission (DPC) against Meta, which declared the data transfers of the service Facebook to the U.S. unlawful and imposed a record fine of EUR 1.2 billion.[14] The case relates to a massive amount of data of EU citizens and touches the foundation of Meta's business model, which can no longer be maintained in the same way after the clear decision of the DPC which orders it to stop the data transfers to the US due to non-compliance with Art. 44 et seq. GDPR. However, the fact that the DPC even ordered Meta to stop the unlawful data transfers for the future and imposed a fine in the first place is solely attributable to the intervention of the EDPB[15], as the DPC had originally rather cautiously only stated the transfers to be contrary to the law in its draft decision. The EDPB, on the other hand, saw the need for a decision on the 'fate' of the data already transferred and the imposition of a fine in view of the seriousness of the violation. In particular, the EDPB emphasised that Meta Ireland by (deliberately) not designing its service in such a way that it could be offered in the EU in a data protection-compliant manner was an indicator that a large part of its revenue was generated precisely because of or based on violations of the

7 See on the question what the adequacy decision now means for controllers and data subjects in the EU the guidance of the EDPB: Europeaan Data Protection Board, 'Information note on data transfers under the GDPR to the United States after the adoption of the adueacy decision on 10 July' (18 July 2023) <https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-data-transfers-under-gdpr-united-states-after_en> accessed 1 July 2023.

8 Ursuala von der Leyen, cited in the Commissions press release, ibid (n5).

9 CJEU, judgment of 16.6.2020, C-311/18 - Facebook Ireland und Schrems, ECLI:EU:C:2020:559.

10 As a counter-example, which shows that US tools can also be used in conformity with data protection law, the final decision of the EDPS on the video conferencing system of the CJEU, issued on 13 July 2023, can be cited (EDPS, 'EDPS Decision on the CJEU's use of Cisco Webex video and conferencing tools' (13.7.2023), <https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/2023-07-13-edps-cjeus-use-cisco-webex-video-and-conferencing-tools_en> accessed 1 July 2023. The main characteristics of the videoconferencing services used by the CJEU which lead the EDPS to approving the use were that no data is transmitted to the cloud for confidential meetings; that very limited data are transmitted to the cloud for other meetings with full and strong encryption (end-to-end encryption, one to many points) by default; that strong technical and organisational measures were included; and that cloud servers located exclusively within the EU are used.

11 BVwG, decision of 12.5.2023, W245 2252208-1/36E, <https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230512_W245_2252208_1_00/BVWGT_20230512_W245_2252208_1_00.pdf> accessed 1 July 2023.

12 See in detail Winklbauer and Horner 'Austrian DPA Decides EU-U.S. Data Transfer Through the Use of Google Analytics to be Unlawful' (2022) 8(1) EDPL 78-84.

13 In France, see the decision of CNIL of 10.2.2022 (<https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf>); in Italy, see decision of GPDP of 9.6.2022 (<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782890>).

14 DPC 'Decision made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation' (12.5.2023), <https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf> accessed 1 July 2023.

15 Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (13.4.2023), <https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_de> accessed 1 July 2023.

GDPR. As was the case with the decision of January 2023 to impose a fine against WhatsApp[16], once again the DPC in its press release shed light on the fact that it does not entirely support the EDPB's decision. There are currently proceedings pending before the General Court and Court of Justice of the Court of Justice of the European Union (CJEU) against various binding decisions of the EDPB in relation to Meta[17], which have been brought by both Meta and the DPC and are seeking (partial) annulment of the decisions. Against this background, it is not unlikely that this decsion will eventually also end up before the General Court, and finally the CJEU in one way or another. In contrast, the public discussion about the DPC investigations, which are often of EU-wide relevance due to the role of the Irish DPA as lead authority over many of the US tech firms, may find it more difficult to find a official and reliable source to rely on in the future. On 28 June 2023, the Irish Parliament passed amendments to the Courts and Civil Law (Miscellaneous Provisions) Bill 2022[18] which, among other things, allow the DPC to declare its proceedings confidential in certain cases, making it a criminal offence to report on them.

Not bound by confidentiality rules, in this edition's Reports Section *Lisette Mustert* takes a closer look at the EDPBs decision in her contribution '**EDPB Decision 1/2023: The Schrems Saga Back on the GDPR's Enforcement Rails**'. In her concluding remarks she states that while it is a welcome development that the Irish DPC was now, finally, urged to adopt a record fine, questions and concerns remain in particular with regard to the discretion that is left to the lead supervisory authority when implementing EDPB decisions. Although the aforementioned pending cases before the CJEU will certainly clarify the scope of the EDPB's powers, they will not change the basic concept of the GDPR concerning lead supervision. However, the issue of more harmonised and effective enforcement is definitely on the Commission's radar. In a (potentially) major step in advancing the GDPR framework, it proposed on 4 July 2023 a Procedural Regulation which aims to set up concrete procedural rules for the authorities when applying the GDPR in cross-border cases, by e.g. obliging the lead supervisory authority to share its views and information earlier and in more detail with its colleagues.[19] In particular, some points from the EDPB's 'wish list'[20] are fulfilled, as with regard to the streamlining of procedural rights. Other problems that have been identified in the first five years of applicability of the GDPR, and although the GDPR's 'landmark' impact and 'future-proofness' are outlined,[21] will probably only be solved within a reform, for which there are certainly also plenty of wish lists and ideas collections.[22]

But already now, the work of or within the EDPB has certainly contributed to a (more) harmonised application of the law, ironing out some of the edges of the GDPR in the process, and the Board continues to be anything but inactive, also under the new Chairwoman and Head of Finnish data protection authority Anu Talis who was elected on 25 May 2023. *Sandra Schmitz-Berndt* provides us in her contribution '**Round-up: Recently Adopted EDPB Guidelines Contextualised**' with exactly that: an round-up of the most recent outcomes from the Board including a contextualisation with its strategy for 2021-2023 and former approaches. She gives us an overview on the EDPB Guidelines on personal data breach notification, on the calculation of administrative fines, on the application of the dispute resolution mechanism and on the use of facial recognition technology in the area of law enforcement, and draws lines to other developments on EU and national level.

16 See DPC 'Data Protection Commission announces conclusion of inquiry into WhatsApp' (19.1.2023), <https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp> accessed 1 July 2023.

17 C-97/23 P *WhatsApp Ireland v EDPB*; T-325/23 *Meta Platforms Ireland v European Data Protection Board*; T-129/23 *Meta Platforms Ireland v European Data Protection Board*; T-128/23 *Meta Platforms Ireland v European Data Protection Board*; T-682/22 *Meta Platforms Ireland v European Data Protection Board*; T-111/23 *Data Protection Commission v European Data Protection Board*; T-84/23 *Data Protection Commission v European Data Protection Board*; T-70/23 *Data Protection Commission v European Data Protection Board*.

18 Courts and Civil Law (Miscellaneous Provisions) Bill 2022, <https://www.oireachtas.ie/en/bills/bill/2022/84/> accessed 1 July 2023.

19 Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final, <https://commission.europa.eu/system/files/2023-07/COM_2023_348_1_EN_ACT_part1_v5.pdf> accessed 1 July 2023.

20 EDPB, Letter to Commissioner Reynders (10.10.2022), <https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf> accessed 1 July 2023.

21 European Commission, 'Statement ahead of the 5th anniversary of the General Data Protection Regulation' (24.5.2023), <https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2884> accessed 1 July 2023.

22 See on this for example the contribution compiled in the EU Law Live Symposium on the 5th Anniversary of the GDPR: Dominik Düsterhaus (ed.), 'Five Candles for the GDPR' (May 2023), <https://eulawlive.com/symposia/5-candles-gor-the-gdpr/> accessed 1 July 2023.

One of these developments, in light of facial recognition addressed by the EDPB, concerns the Olympic and Paralympic Games in 2024. Since organiser France has decided to monitor the security of these (and other) major events with the help of algorithm-driven video surveillance, among other things, the Games are eagerly awaited not only by sports fans but also by those interested in data protection law. For the latter, however, the anticipation might have already reached its peak with the decision of the French Constitutional Council, which approved (with a few restrictions) the respective elements of the proposed 'Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres disposition' that have been widely criticised from the perspective of privacy protection. *Hugo Lami* guides us through the comprehensive decision in his contribution '**The Constitutional Council Validates the Use of Augmented Video Recognition Technology for the Olympics**'. In particular, however, the author focuses on which protective mechanisms the French law provides for the using of algorithmic technologies and puts these and other legislative developments in France (for example, on the use of facial recognition in public places) into context in terms of their significance for the AI Act[23] proposed at the EU level.

These issues could not be more topical and urgent, as the adoptions of the final negotiating positions by the European Parliament[24] and the Council[25] at the EU level have cleared the way for the legislative trilogue on the AI Act. An adequate protection of the right to personal data protection and the relationship to the GDPR in the regulation of AI are just two of many topics on the negotiation agenda. In the meantime, the search for compromise on another EU legal instrument with significant cross-references to data protection law have come to a successful conclusion: On 12 July 2023, the European Parliament and the Council signed a Regulation and a Directive on cross-border access to electronic evidence marking the completion of a five year legislative process. We are grateful for being able to include an 'on-the-minute' contribution by *Stanislaw Tosza* in this edition's Reports Section asking: '**The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?**'. The author unpacks the e-evidence package and sheds light on its background including an assessment on which impact the adopted rules will have and where challenges most likely will arise in the future implementation. As *Tosza* points out, the package will become fully applicable only in three years and its efficiency will depend on several factors, which are still open in the legislation itself. This comprehensive report is therefore certainly not the last we will hear on the subject of electronic evidence in the scope of the EDPL.

This might also apply to the third regulation which we are taking a closer look at in this issue. Since neither the Council nor the Parliament have found their final negotiating positions on it yet, the proposal for a regulation laying down rules to prevent and combat child sexual abuse (referred to as CSAR or CSAM Proposal) is far less advanced in the legislative process than the AI Act and obviously the e-evidence package, but no less controversial. The main point of contention is the question of conformity of the envisaged system of detection orders against hosting and interpersonal communication services, which is being discussed under the heading of 'chat surveillance', with EU law. The fact that Parliament and Council are not confident about the answer to this question is demonstrated by studies commissioned by both institutions, the findings of both the Research Service and the Legal Service being highly critical. *Teresa Quintel* gives us an insight in her contribution '**Renewed Concerns about Compliance of the proposed 'Regulation to Prevent and Combat Child Sexual Abuse' with Essence of Right to Data Protection: The Council Legal Service Opinion**', which deals intensively with the controversy surrounding chat surveillance and other aspects of the proposal. She not only sheds light on (data protection) law-related points of criticism, but also on their interplay with the existing technical framework conditions, which the proposal, despite its noble goals, cannot ignore. Her comments on safeguards foreseen, issues of end-to-end-encryption, the taxonomy of abuse material, possible scope of effectiveness and law enforcement issues, do not raise much hope for

23 Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final.

24 P9_TA(2023)0236, Amendments adopted by the European Parliament on 14 June 2023, <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> accessed 1 July 2023.

25 ST 15698 2022 INIT, General Approach adopted on 6 December 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_15698_2022_INIT> accessed 1 July 2023.

a quick and/or satisfactory conclusion of the legislative process.

In the context of questions of uniform application and enforcement of the GDPR, three contributions in this Reports Section deal with decisions of national data protection authorities, each of which addresses issues that are likely to be relevant in all Member States.

A good example is the report by *Katharina Kollmann*, entitled '**Reconciling 'Pay or Okay' Models with the GDPR: The Austrian DPA Decision and other Recent Approaches in Europe**', which deals with a globally widespread financing model of online offerings – many of our readers from different Member States will no doubt have stumbled across pop-up windows while surfing the Internet that presented them with the choice of 'accepting cookies' or 'paying for subscription' before they could access particular content. *Kollmann* focuses on a decision by the Austrian data protection authority on the model of paying with data in exchange for access to news content, but also highlights recent approaches by the Danish and German data protection authorities. In her comparison, she concludes that although all authorities consider so-called pay-or-okay models to be permissible in principle under data protection law, also with regard to the basic idea of payment with data from the Digital Content Directive[26], other priorities and criteria are applied in each of the approaches.

The decisions of the Maltese authority in the context of the (unlawful) processing of voter data of almost the entire population of Malta are not only supranationally relevant, but also attracting supranational attention. In their report '**Maltese DPA rules on Data Breach involving an Illegal Voter Database and the Right of Access**' *Mireille M. Caruana* and *Roxanne Meilak Borg* report on a case involving a database with particular sensitive data on political leanings, a cybersecurity incident, 'undetermined' sources of data collection and unsuccessful access requests, which now led to a high fine of EUR 65.000 in the EUs smallest Member State.

While the fine imposed in the case *Giorgia Bincoletto* reports about was not so high, the underlying context of it certainly is important. Her contribution '**Italian DPA fined Condominium Manager for the Disclosure of Covid-19 Positivity in the Building**' deals with a decision that once again shows that data protection compliance does not stop at everyday situations (disclosure of Covid 19 status of a family to fellow residents by a facility manager) and that even processors acting with the best intentions (containment of the risks) have to comply with these principles. In particular, they cannot rely on the protection provided by the household exemption or the defence of pursuing legitimate interests when it comes to special categories of personal data (health data). *Bincoletto* also points to the different approaches taken by Member States in justifying and evaluating pandemic mitigation measures under data protection law leading to divergences in harmonisation.

Another matter relating to facility management is dealt with in the decision of the Finnish Supreme Administrative Court from a data protection perspective, which *Päivi Korpisaari* reports on. Although, it has a completely different focus. A rental company collected the personal identity numbers of all family members, including children, living in or applying for accommodation in their buildings. The Finnish data protection authority set clear limitations for this type of data collection and was now confirmed by the Court. In her contribution '**Supreme Administrative Court of Finland on Processing of Children's Data in Light of the Principle of Data Minimisation**' our Finnish correspondent deals in detail with the Court's elaborations on the principle of data minimisation as laid down in in Article 5(1)(c) GDPR and its importance with regard to processing data of minors, which need special protection.

The circle of the Reports Section, which we opened by our introductory remarks on data transfers outside the EU and their significance for business operations in and from the internal market, closes with the two international contributions that deal with developments in data protection law outside the EU which need to be seen in light of the GDPRs spillover or 'Brussels effect'.

The contribution from the UK may not really seem 'outside the EU' at first - after all, the UK has so far adhered to the legal framework of the GDPR with only a slightly adapted UK GDPR and could therefore seamlessly continue previous data processing as usual under the framework of an adequacy decision. However, the UK government now wants to break

26 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

new ground. The reform of the data protection framework within the Data Protection and Digital Information Bill, which has been discussed for some time, is now in its 'Version 2' at report stage in the House of Commons, and is intended to become law sometime before March 2024. It is significant, because it would be the first situation in which a state does not move closer to GDPR standards, but having been previously bound by these, would decide to move further way in the future. *Luben Roussev* reports on the fine line between aiming for greater 'business friendliness', in particular by reducing regulatory burdens for non-risky processing operations, and the desire to remain as a safe third country with an adequate level of data protection under GDPR. Under the heading '**The DPDI No.2 Bill - GDPR Revamp or Rule Tinkering?**' he points to and explains the key aspects of the reform – clarifying definitions, rules on automated decision-making, removing regulatory burdens and reforming supervisory structures as well as the concept of data protection officers – and asseses how these developments interact with the EU model, especially in light of international data transfers.

Last but not least, as also the reports from Finland and on the CSAM Proposal underline, there is an increasing development on minor-specific protections developed in legislation and regulatory practice across the world. An example outside of data protection but related to it, is the sector of media and platform use, concerning which we had the possibility to recently co-author an extensive comparative study covering the developments and status of international child and youth media protection.[27] In our Practitioners' Corner of this edition we have a comparable comparative approach to a report which considers how not only the GDPR deals with minors and the processing of their data with specific norms, but also diverse and divergent jurisdictions such as China, California and Australia. These increasingly complex layers of rules addressing minors – another example would be the DSA's[28] Article 28 on the online protection of minors – necessitates careful consideration in companies providing online services which are within the scope of these norms. It seems advisable for them to foresee compliance officers or units for the specific category or subject matter of minors, similarly as is the case in some national media laws that require the nomination of a protection of minors officer in media companies overseeing specifically how the safety of this age group is considered in the daily business of the provider. The report '**Influence of the GDPR on Protection of Young People's Privacy: New developments in China, California and Australia**' authored by *Normann Witzleb* and *Sarah Hünting* is aimed at underscoring this high practical relevance at least for a number of companies that may so far not have even considered the need for specific attention to these questions. Furthermore it elaborates on the fact how these developments were influenced by approaches in the EU.

This overview of our, this time particularly packed, Reports Section hopefully demonstrates not only the relevance of the topics covered, but also their timeliness – both of which we can provide thanks to our country and topical 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>.

27 Jörg Ukrow, Mark D. Cole and Christina Etteldorf, 'Stand und Entwicklung des internationalen Kinder- und Jugendmedienschutzes' (2023) German, but with an extensive Executive Summary in English, available at <https://www.dco-verlag.de/wis/ebk/9783910513129.pdf> accessed 1 July 2023.

28 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.