EDITORIAL

Privacy in Challenging Times*

Phew! 2020 is (finally) over and, to say the least, it has been an extremely difficult year. The COVID-19 pandemic has changed the way in which we live our lives and it is by no means over. Nevertheless, it is important to remain positive and this editorial note is a hopeful one. Despite the tragedy of the COVID-19 pandemic, there have been humanitarian developments worth celebrating and in many ways this truly global event has brought us closer together, given us a different perspective on life and reinforced the value of good health. Lessons in democracy and freedom have also been learnt in 2020, two matters which are often taken for granted in the West.

There have also been a number of developments in privacy to celebrate. As highlighted in the European Commission's first evaluation report in 2020 (widely viewed as the world's 'gold standard' for the protection of personal data) the General Data Protection Regulation (GDPR) itself has[1,2]:

> strengthened data protection safeguards, provides individuals with additional and stronger rights, increased transparency, and ensures that all those that handle personal data under its scope of application are more accountable and responsible. It equips the independent data protection authorities with stronger and harmonised enforcement powers and sets up a new governance system. It also creates a level playing field for all companies operating in the EU market, regardless of where they are established, and it ensures the free flow of data within the EU, thereby strengthening the internal market.

Since the GDPR took effect, global data privacy has shifted its focus from *soft law* to stepped-up enforcement.[3] Its adoption has spurred other countries in many regions of the world to consider following suit, including Brazil, Chile, India, Indonesia, Japan,[4] Kenya, South Korea, and the US (California).[5] 2020 has seen an increased awareness of data protection and privacy rights, driven by countless GDPR public awareness campaigns, harsh enforcement actions and fines. All of these have resulted in the enactment of numerous laws and regulations enacted across the globe.

The California Consumer Privacy Act (CCPA), the first major US privacy legislation, entered into force in 2020. Similar to the GDPR globally, the CCPA has inspired other states in the US (Hawaii, Massachusetts, New Jersey, Pennsylvania, Rhode Island, and Washington) to propose privacy bills.[6] In 2021, we may finally see the long-awaited US federal privacy law, which would address how companies handle consumer data, based on the CCPA model.[7]

Uncertainty over international data transfers has troubled 2020, particularly with the Court of Justice of the European Union (CJEU) striking down the EU–US Privacy Shield.[8] Nevertheless, the CJEU upheld the

Notes

* Special thanks to Andrew Poulton (Linklaters, London) for reviewing this editorial note. All errors, of course, remain mine.

1 European Commission, Communication from the Commission to the European Parliament and the Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, SWD(2020) 115 final 1 (24 June 2020), https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf (accessed 24 Dec. 2020).

2 Tanguy Van Overstraeten & Ceyhun Necati Pehlivan, *The EU Commission Publishes Its First Evaluation of the GDPR*, Linklaters Digilinks Blog (7 July 2020), https://www.linklaters.com/en/insights/blogs/digilinks/2020/july/the-eu-commission-publishes-its-first-evaluation-of-the-gdpr (accessed 24 Dec. 2020).

3 PwC, *Top Policy Trends 2020: Data privacy – California*, https://www.pwc.com/us/en/library/risk-regulatory/strategic-policy/top-policy-trends/data-privacy.html (accessed 24 Dec. 2020).

4 *See* 1 Global Privacy Law Review 126–189 (Kluwer Law International 2020), Japan special issue.

5 European Commission, *supra* n. 1, at 3.

6 PwC, *supra* n. 3.

7 Washington Post Editorial Opinion, *Dear Congress: Stop Promising a Federal Privacy Law. Pass One Instead* (16 Dec. 2020), https://www.washingtonpost.com/opinions/dear-congress-stop-promising-a-federal-privacy-law-pass-one-instead/2020/12/15/2fd7a3b2-3e4f-11eb-9453-fc36ba051781_story.html (accessed 24 Dec. 2020).

8 *See infra* nn. 69 and 70.

validity of standard contractual clauses (SCCs) and a pathway for such international transfers remain. Data exporters and importers must assess, prior to any transfer, the laws of the third country to which data is transferred to determine if those laws ensure an adequate level of protection of personal data.[9] The practical implications of *Schrems II* remain unclear for both companies and EU data subjects.

It is also important to celebrate the achievements and successes of this publication. At Global Privacy Law Review (GPLR), we delivered three issues in 2020 comprising more than twenty academic articles, professional reports, opinions, case notes, and news written by first class scholars, researchers and professionals. Only in a year's time, we have had subscribers and readers join us from all around the world. We are truly a 'global law' review. Our Editorial Board celebrate this achievement and we undertake to continue delivering top-quality content and research to you.

On this note, I am delighted to start this year's volume again with excellent and innovative research papers, articles and case notes.

First, under the *Articles* section, Prof. Boris P. Paal (*Market Power in Data (Protection) Law*) analyses the interesting relationship between data protection and antitrust laws.[10] In particular, he discusses how the traditional antitrust law concept of 'dominant position' in the digital economy market (especially relevant for Big Tech) may have effects under data protection law.

Paal examines the effects of such a dominant market position on the lawful grounds provided under Article 6 GDPR. He argues that, when processing personal data on the basis of consent,[11] it is necessary to consider the potential dominant market position of a data controller.[12]

Under the GDPR, consent must be freely given, specific, informed and unambiguous.[13] As the European Data Protection Board (EDPB) states[14]:

> The element 'free' implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.

A lack of 'free' or 'real choice' can be typically found where an 'imbalance of power' exists between the controller and the data subject.[15] Accordingly, Paal argues that the dominant market position of a data controller should be taken into account when determining whether or not a user's consent was 'freely given' under the GDPR.[16] An 'imbalance of power' could exist when the data subject is dependent on the very service of the controller and no adequate alternatives are available.[17] Conversely, the 'free' nature of the consent of a data subject would be presumed when there is a comparable offer on the market, especially when available offers are data privacy-friendly.[18] Paal concludes however that a clear imbalance of power is only an indication of a potential lack of real choice for data subjects, and is not sufficient in itself to determine whether the consent was freely given.[19] Freedom of choice must be addressed in the light of the specific circumstances.[20]

In relation to the processing of personal data on the grounds of the necessity for the performance of a contract[21] or the balancing of legitimate interests,[22] Paal considers that the potential dominant market position per se would not be a determining factor.[23]

In its landmark decision of 7 February 2019, the German Competition Authority *Bundeskartellamt* prohibited Facebook from using terms of service that force users to consent to Facebook collecting personal data from third-party websites and apps (including Facebook-owned services) and assigning these data to the users' Facebook accounts.[24] Facebook's dominant market power and the corresponding power to unilaterally impose terms

Notes

[9] Tanguy Van Overstraeten & Ceyhun Necati Pehlivan, *EU: EDPB publishes FAQs Following the Schrems Judgment*, Linklaters Digilinks Blog (27 July 2020), https://www.linklaters.com/en/insights/blogs/digilinks/2020/july/eu—edpb-publishes-faqs-following-the-schrems-judgment (accessed 24 Dec. 2020).

[10] Boris P. Paal, *Market Power in Data (Protection) Law*, in this issue, at 8.

[11] Art. 6(1)(a) GDPR.

[12] Paal, *supra* n. 10, at 14.

[13] Art. 4(11) GDPR.

[14] EDPB, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, 7 (4 May 2020).

[15] Recital 43 GDPR; EDPB, *supra* n. 14.

[16] Paal, *supra* n. 10, at 10.

[17] *Ibid.*, at 12.

[18] *Ibid.*, at Ibid.

[19] *Ibid.*, at 14.

[20] *Ibid.*, at 12.

[21] Art. 6(1)(b) GDPR.

[22] Art. 6(1)(f) GDPR.

[23] Paal, *supra* n. 10, at 12.

[24] Bundeskartellamt, *Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing*, Case Summary (15 Feb. 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (accessed 23 Dec. 2020); Marco Botta & Klaus Wiedemann,

of service on its users also played a significant role for this outcome.[25] *Bundeskartellamt* stated[26]:

> [T]he purpose of [the data protection law] is to counter asymmetries of power between organisations and individuals and ensure an appropriate balancing of interests between data controllers and data subjects. In order to protect the fundamental right to informational self-determination, data protection law provides the individual with the right to decide freely and without coercion on the processing of his or her personal data. …
>
> [I]n view of Facebook's dominant position in the market, users consent to Facebook's terms and conditions for the sole purpose of concluding the contract, which cannot be assessed as their free consent within the meaning of the GDPR.

Accordingly, *Bundeskartellamt* concluded that only 'voluntary consent' can serve as a lawful basis (cf. Article 6(1)(a) GDPR), and voluntary consent to a data subject's information being processed cannot be assumed if their consent is a prerequisite for using the Facebook service in the first place.[27] While the German Federal Court of Justice *Bundesgerichtshof* upheld the *Bundeskartellamt*'s decision during interim proceedings on 23 June 2020,[28] *Bundesgerichtshof* did not have to decide whether or not acceptance of Facebook's terms of service would fulfil the GDPR requirements relating to consent.[29]

Second, Dr Nicolas Anciaux, Prof. Célia Zolynski, Sébastien Chaudat & Riad Ladjel (*Empowerment and Big Personal Data: from Portability to Personal Agency*) propose implementing the concept of 'personal agency' in the Big Data context as a mean to 'empower individuals'.[30] Based on the sociological concept of 'agency', which may be defined as the capacity of individuals to act independently and to make their own free choices, Anciaux et al. propose that all individuals should be able to make decisions about their own data and become an 'agent' of the way their decisions are implemented.[31]

Anciaux et al. argue that the 'empowerment of the individual' notably stem from a number of data subject rights, in particular the GDPR's right to the portability of personal data.[32] This new right led to the design and deployment of technical platforms, such as personal cloud, personal server, or personal information management systems (PIMS), which give individuals more control over their personal data.[33] PIMS would allow individuals to control their personal data and manage their online identity by enabling them to collect, store, update, and share personal data.[34] They also let users allow, deny, or withdraw consent to third-parties for access to their personal data.[35] Such tools would allow individuals to consolidate their data in a single system managed under their control.[36]

However, the authors argue that the implementation of the portability right through PIMS is not sufficient, and additional mechanisms to give user controls over data portability procedures are needed.[37] By means of what they call 'personal agency', they propose giving individuals an active role and control over the lifecycle of their personal data, from collection to destruction, and enabling them to make decisions (and also take responsibility) in relation to how their own data are managed. This would open up a new reading of the empowerment measures on Big Data functionalities on personal data.[38]

Third, Yves Bauer, Prof. Nathalie Tissot, Prof. Bertil Cottier & Dr Hugues Mercier (*Is a Relative Definition of the Notion of Erasure the Much Sought-after Solution to the Dilemma Between Robust Integrity and Total Eradication?*) highlight the tension that wavers between the GDPR's security and data minimization principles.[39]

Notes

Exploitative Conducts in Digital Markets: Time for a Discussion After the Facebook Decision, 10 J. Eur. Competition L. & Prac. 465 (2019), https://journals.sagepub.com/doi/10.1177/0003603X19863590 (accessed 23 Dec. 2020).

[25] Botta & Wiedemann, *supra* n. 24.

[26] Bundeskartellamt, *supra* n. 24, at 8 & 10.

[27] *Ibid.*, at 11.

[28] Case KVR 69/19, *Bundesgerichtshof*, *Bundeskartellamt v. Facebook*, 23 June 2020, ECLI:DE:BGH:2020:230620BKVR69.19.0.

[29] Klaus Wiedemann, *A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)*, 51 Int'l Rev. Intell. Prop. & Competition L. 1168 (Springer 2020), https://link.springer.com/article/10.1007/s40319-020-00990-3#Fn36 (accessed 23 Dec. 2020).

[30] Nicolas Anciaux et al., *Empowerment and Big Personal Data: from Portability to Personal Agency*, in this issue, at 16.

[31] *Ibid.*, at 21.

[32] *Ibid.*, at 16.

[33] *Ibid.*, at Ibid.

[34] IAPP, *Personal Information Management Systems: A New Era for Individual Privacy?* (21 Mar. 2019), https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy/ (accessed 24 Dec. 2020).

[35] *Ibid.*

[36] Anciaux et al., *supra* n. 30, at 16.

[37] *Ibid.*, at 18.

[38] *Ibid.*, at 16.

[39] Yves Bauer et al., *Is a Relative Definition of the Notion of Erasure the Much Sought-After Solution to the Dilemma Between Robust Integrity and Total Eradication?*, in this issue, at 31.

The authors note that the implementation of state-of-the-art technologies offers promising opportunities for data controllers to ensure the security of the personal data they process, particularly in relation to availability and accuracy.[40] However, they argue that such technologies may also enter into conflict with other GDPR requirements, especially regarding the erasure of personal data at the end of the life-cycle of data or when requested by the data subject.[41] In particular, such conflicts may arise when some technologies such as blockchain[42] or data entanglement[43] are used.

Bauer et al. note that erasure should 'be as inevitable and as irreversible as death, whether abrupt through the exercise of a right [to erasure], or more peacefully, at the end of its life cycle'.[44] However, they note that the concept of 'erasure' is not clearly defined under the GDPR, and its interpretation shall not be limited to the physical destruction or *hard deletion* of the personal data.[45] They argue that, when technical measures implemented for the purpose of ensuring security or availability of the personal data do not allow for its physical destruction, 'relative erasures' should be sufficient to comply with data erasure requirements under the GDPR.[46] Such relative erasures would consist of processing activities that put personal data beyond use in a way that makes it impossible, for the controller or third parties, to process it again without disproportionate efforts.[47]

Bauer et al. suggest that such a *relative* interpretation of the notion of 'erasure' would allow data controllers, who implement strong technical measures to ensure security and availability of the personal data, to comply with the GDPR. Combined with a careful design of privacy, it may ensure the data subject's rights without requiring detrimental security concessions.[48]

Fourth, Dr Mariusz Krzysztofek (*The Interpretation of 'Household' in the Definition of Personal Information in the CCPA*) explores the interpretation of 'household' in the definition of 'personal information' set out under the CCPA.[49]

The CCPA, the first major US privacy legislation, came into force on 1 July 2020. It gives California consumers more control over the personal information that businesses collect about them. The CCPA defines personal information as any information that identifies, directly or indirectly, with a particular consumer or *household.*[50] For example, personal information could include a consumer's name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about their preferences and characteristics.[51]

However, Krzysztofek argues that the interpretation of 'household' within the definition of a consumer's personal information remains unclear.[52] He notes that since even a person living alone in a housing unit is counted as a household, it is not clear how an individual within a household differs from a consumer in the definition of personal information.[53] In other words, those persons who constitute a household are at the same time consumers as defined in the CCPA (i.e. California residents), and a reference to 'household' would duplicate the meaning of 'consumer' in the definition of personal information.[54]

The guidance of the CCPA issued by the Office of the Attorney General actually shows that at the end of the day, the household needs to be tied to a consumer in order to validate the request.[55] For example, the guidance at § 999.318 also explicitly refers to 'all consumers of the household'.[56]

According to Krzysztofek, the scope of the definition of personal information and therefore the scope of the CCPA become uncertain without answering the question of how 'household' is to be understood in the CCPA.

Notes

[40] *Ibid.*, at 31.

[41] *Ibid.*, at 36.

[42] Ceyhun Necati Pehlivan & Inés Isidro, *Blockchain and Data Protection: A Compatible Couple?*, 1 Global Privacy L. Rev. 39, 46–47 (2020).

[43] James Aspnes et al., *Towards a Theory of Data Entanglement*, 389 Theoretical Computer Sci. 26 (2007).

[44] Bauer et al., *supra* n. 39, at 36.

[45] *Ibid.*, at 33.

[46] *Ibid.*, at 37.

[47] *Ibid.*, at 37.

[48] *Ibid.*, at 31.

[49] Mariusz Krzysztofek, *The Interpretation of 'Household' in the Definition of Personal Information in the CCPA*, in this issue, at 38.

[50] CCPA, s. 1798.140 (o) (1).

[51] CCPA, s. 1798.140 (o) (1) (A) to (K).

[52] Krzysztofek, *supra* n. 49, at 38.

[53] *Ibid.*, at 39.

[54] *Ibid.*, at 41.

[55] *Ibid.*, at 43.

[56] *Ibid.*, at 40.

Consequently, he proposes deleting the reference to 'household' in future amendments of the CCPA.

Fifth, Arvin Kristopher A. Razon (*Are Narco-Lists Covered by the Philippine Law On Privacy? Exploring the Limits of the 'Classic' Right to Privacy and Applying a Constitutionally Grounded Data Protection Right*) examines the limits of the right to privacy recognized under the Philippine constitution, and the constitutional underpinnings of the right to data protection, in the context of 'narco-lists' or 'intelligence reports' issued by Philippine President Rodrigo Duterte.[57]

Since taking office on 30 June 2016, President Duterte has carried out a 'war on drugs', which, according to a UN report, has led to the deaths of thousands of Filipinos to date, raising human rights concerns.[58]

During his presidency, Duterte administration has released several narco-lists, containing names of public officials and politicians allegedly involved in illegal drugs.[59] Duterte further stated[60]:

> An official's right to privacy is not absolute and there is a compelling reason to prioritize the state and the people. As your president, my ultimate concern is the pursuit of order in government.

Razon notes that whether individuals named in the narco-lists would be successful in asserting the *right to privacy* against the release of such narco-lists is uncertain because of their decreased expectation of privacy, their status as public figures, and the countervailing rights to be balanced.[61]

Nonetheless, Razon conceptualizes the *right to data protection* as a constitutional right, and argues that this right may be asserted by individuals named in the narco-lists.[62] He argues that, consequently, individuals should be able to either require the government to comply with *ex-ante* protections or exercise their rights to reasonable access, rectification, erasure or blocking, and damages.[63]

Sixth, Assoc. Prof. Leyla Keser Berber & Ayça Atabey (*Open Banking & Banking-as-a-Service (BaaS): A Delicate Turnout for the Banking Sector*) examine open banking & Banking-as-a-Service (BaaS), including applicable regulatory requirements under the EU Payment Services Directive (PSD2) and the GDPR.[64]

Keser & Atabey note that digitalization has prompted the adoption of innovative strategies and transformation in the banking sector. They explain the difference between open banking and platform banking and touch upon the opportunities that platform banking may provide for the banking sector while underscoring the implications of the triggers stemming from regulatory trends in the financial industry.[65]

In the context of open banking and platform banking, Keser & Atabey provide an overview of the legal framework applicable in the EU, more specifically, the PSD2 and GDPR.[66] They also explain the recent developments in Turkey relating to open banking regulation.[67]

The authors conclude that banks should pay close attention to regulatory implications of open banking and BaaS and use them to their advantage, while making data protection and privacy considerations one of the priorities in practice to invest in building trust, which serves as a basis of financial services.[68]

Seventh, under the *Case Note* section, Dr Joshua P. Meltzer (*After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals*) examines the recent landmark ruling of the CJEU, the so-called 'Schrems II' decision.[69,70]

The CJEU has recently invalidated Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield,[71] citing concerns that US intelligence agencies can access personal data relating to EU residents in ways that are incompatible

Notes

[57] Arvin Kristopher A. Razon, *Are Narco-Lists Covered by the Philippine Law On Privacy? Exploring the Limits of the 'Classic' Right to Privacy and Applying a Constitutionally Grounded Data Protection Right*, in this issue, at 44.

[58] BBC News, *Philippines Drugs War: UN Report Criticises 'Permission to Kill'* (4 June 2020), https://www.bbc.com/news/world-asia-52917560 (accessed 24 Dec. 2020).

[59] Rambo Talabong, *Duterte Releases Drug List Ahead of 2019 Elections*, Rappler (14 Mar. 2019), https://www.rappler.com/nation/elections/duterte-releases-drug-list-ahead-of-2019-elections (accessed 24 Dec. 2020).

[60] *Ibid.*

[61] Razon, *supra* n. 57, at 58.

[62] *Ibid.*, at Ibid.

[63] *Ibid.*, at 55 & 56.

[64] Leyla Keser Berber & Ayça Atabey, *Open Banking & Banking-as-a-Service (BaaS): A Delicate Turnout for the Banking Sector*, in this issue, at 59.

[65] *Ibid.*, at 60.

[66] *Ibid.*, at Ibid.

[67] *Ibid.*, at 76 et seq.

[68] *Ibid.*, at 60.

[69] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (16 July 2020) ECLI:EU:C:2020:559.

[70] Joshua P. Meltzer, *After Schrems II: The Need for a US–EU Agreement Balancing Privacy and National Security Goals*, in this issue, at 83.

[71] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield, C(2016) 4176, OJ L 207, 1–112 (1 Aug. 2016).

with EU personal data protection laws and because EU residents lack proper enforcement rights in respect of their personal data.[72]

According to Meltzer, the issues at stake in Schrems II around privacy on the one hand and how governments access data for national security purposes on the other reflects a broader tension between the globalized internet, the free flow of data, and national laws and goals.[73]

Meltzer also questions the consistency of the surveillance laws and practices of the Member States bound by the Schrems II ruling.[74] He argues that giving EU Member States greater discretion to balance national security needs with privacy standards than the US would be unsustainable.[75] He considers that the US needs to take the lead in setting out a model that effectively balances the needs and practices of national security agencies with rights to privacy.[76]

Meltzer concludes that finding common ground is essential if the US and the EU are to make progress forging a partnership on other areas of data governance and digital trade, including on how to regulate technologies such as AI.[77]

Last but not least, Emmanuel Ronco, Natascha Gerlach, & Natalie Farmer from Cleary Gottlieb Steen & Hamilton LLP *(Recommendations of the EDPB Further to the CJEU's Schrems II Judgment: One Step Forward, Two Steps Back?)* examine the recommendations of the EDPB[78] (Recommendations) following the Schrems II judgment.

Ronco, Gerlach & Farmer note that the Recommendations in their current form create legal uncertainty and are likely to lead to inconsistency and a lack of transparency for data subjects. They argue that requiring data exporters and importers to assess whether personal data may be safely transferred to certain third countries and under what conditions would place an undue burden on data exporters and importers. Further, this would discourage the transfer of data to countries simply because their surveillance laws and practices are not transparent, force the repatriation of data hosted using cloud service providers to EU-based servers, which may offer lesser security standards, and overly focus on encryption as the sole effective technical measure when transferring data to third countries through cloud computing services or remote access, ignoring other measures such as pseudonymization which could increase the level of protection of the data.[79]

They conclude that the Recommendations depart from the approach to data protection enshrined in the GDPR in various ways and leave data exporters with no way of being able to confidently transfer personal data in a manner that is vital to international commerce.[80]

Ronco et al. recommend that, before issuing the final version of the Recommendations, the EDPB should look for ways to align the fundamental approach more closely with the GDPR, as well as the new SCCs issued by the European Commission.[81]

I hope you enjoy the read. I wish you a brighter and more hopeful 2021.

Ceyhun Necati Pehlivan
Editor-in-Chief

Notes

[72] Ceyhun Necati Pehlivan, *After the Banquet and Beyond: Privacy and Data Protection in Japan*, 1 Global Privacy L. Rev. 126, 127 (2020).

[73] Meltzer, *supra* n. 70, at 89.

[74] *Ibid.*, at 83.

[75] *Ibid.*

[76] *Ibid.*

[77] *Ibid.*, at 89.

[78] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (10 Nov. 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 24 Dec. 2020).

[79] *Ibid.*, at 91.

[80] *Ibid.*, at 100.

[81] *Ibid.*, at Ibid.