The GDPR

Tombal, Thomas

Published in:
Deep diving into data protection

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

The GDPR: A Shield to a Competition Authority's Data Sharing Remedy?

Thomas Tombal[1]

Abstract

Our European economy runs on data, which has become an essential resource for economic growth, job creation and societal progress, and data sharing is often presented as the avenue forward to reap such benefits. This call for more data sharing might create tensions with the personal data protection rules. Yet, these policy objectives are not incompatible and the challenge is thus not whether one should prevail over the other, but rather how they can be reconciled. Interestingly, privacy and the GDPR are more and more used as a shield to data sharing by incumbent data holders. Yet, if specific circumstances are met, this refusal could amount to a competition law infringement. In this context, providing access to a competitors' data as a remedy to such infringement could therefore be seen as a pro-competitive solution entailing more data sharing. Nevertheless, some of the data at hand could be personal data and some tensions might emerge between competition law and personal data protection law. Therefore, this chapter analyses how a competition authority's decision imposing to share personal data with a competitor can be compatible with the GDPR. This requires, on the one hand, to have a lawful basis for the data sharing and, on the other hand, to comply with the general principles of personal data protection. Moreover, competition and data protection authorities will need to collaborate in order to define and implement this remedy.

[1] University of Namur, Faculty of Law, CRIDS/NaDI. The author would like to thank Prof. Cécile de Terwangne and Prof. Alexandre de Streel for their valuable comments on the previous versions of this contribution.

Introduction

1. Our European economy runs on data, which has become an essential resource for economic growth, job creation and societal progress[2], and data sharing is often presented as the avenue forward to reap such benefits[3]. To support its data sharing policy, the European Commission has chosen to rely on contractual freedom and to propose key principles for the undertakings wishing to engage in B2B data sharing agreements[4]. In addition to the formulation of these principles, the Commission has also worked on more concrete recommendations regarding the contractual stipulations that should ideally appear in such agreements[5].

This call for more data sharing might create tensions with the policy objective of the General Data Protection Regulation[6] (hereafter "GDPR"), as one of its aims is to provide more control to the data subjects on the personal data[7] concerning them. Indeed, the data sharing agreements mentioned above will often cover both personal and non-personal data mixed in the same dataset[8], and favouring data sharing might lead to the dissemination of such personal data, consequently reducing the data subjects' control on what happens with "their" data. Though some tensions might emerge between these two policy objectives, they are not incompatible, and sharing personal data can be beneficial for society, governments, undertakings and individuals[9]. The challenge is thus not whether one should prevail over the other, but rather how they can be reconciled[10]. To do so, guidance can be sought in the data sharing code of practice of the Information Commissioner's Office[11], the United-Kingdom's

[2] European Commission (2017), p. 2.
[3] European Commission (2018a).
[4] European Commission (2018a), p. 10.
[5] European Commission (2018b), pp. 6-8.
[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1.
[7] "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier" (Art. 4.1 GDPR).
[8] See Graef et al. (2018) and Wendehorst (2017), pp. 329-330.
[9] Information Commissioner's Office (2019), p. 13.
[10] Muralidhar et al. (2014), p. 2.
[11] Information Commissioner's Office (2019).

data protection authority, and it could be resorted to privacy preserving technical mechanisms[12].

Moreover, some pieces of European legislation already provide for data sharing mechanisms that are compatible with personal data protection rules. For instance, Article 20 GDPR grants two types of personal data portability rights to data subjects. While Article 20.1 GDPR provides that the data subject has the right to receive the personal data which (s)he has provided to a controller in a structured, commonly used and machine-readable format and to transmit it to another controller without hindrance, Article 20.2 GDPR provides that the data subject also has the right to have the personal data transmitted directly from one controller to another, if (s)he has consented to such an operation and if this is technically feasible.

Additionally, it can be argued that the revised Directive on payment services in the internal market (PSD2)[13] has introduced a specific data portability rule in the banking sector[14]. Indeed, PSD2 allows the providers of payment initiation service and the providers of account information service[15] to have access to the payment account information[16] of the users of their services (the consumers) if the latter have explicitly consented to such access[17]. This is a sector-specific application of Article 20.2 GDPR, as it compels the banks to make this direct transmission of the data subjects' personal banking information to recipients technically feasible. This is the main difference with Article 20.2, which contains no such technical feasibility obligation. However, the scope of the sharing mandated by PSD2 is limited to the two scenarios of payment initiation and account information, whereas Article 20 of the GDPR applies generally to all types of services.

2. However, data sharing will not always be voluntary. Indeed, a potential consequence from the Commission's choice to rely on contractual freedom could be that some undertakings are not able to access

[12] See, for instance, Muralidhar et al. (2014).

[13] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ [2015] L 337/35.

[14] Colangelo and Borgogno (2018), p. 3; Vezzoso (2018), pp. 12-13.

[15] Respectively defined as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider" and as "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider" (Directive 2015/2366, art. 4.15 and 16).

[16] Defined as "account held in the name of one or more payment service users which is used for the execution of payment transactions" (Directive 2015/2366, art. 4.12).

[17] Directive 2015/2366, arts. 64-67.

certain data at all[18], because data holders might start refusing to provide access to their data to undertakings with limited bargaining power. In fact, they might even use data protection considerations to justify this refusal, and the dynamic nature of the notion of personal data makes it difficult to evaluate the legitimacy of such claims[19]. Indeed, privacy and the GDPR are more and more used as a shield to data sharing by incumbent data holders such as the GAFAMs. This creates the paradoxical situation in which a tool that was allegedly adopted to restrict these incumbents' power on data, by empowering the data subjects, is actually used by these incumbents in order to raise entry barriers on the data market vis-à-vis third parties. Yet, under EU competition law, if an undertaking holding a dominant position refuses to grant access to its data to another undertaking, this could potentially lead to the application of the Essential Facilities' case law[20] and to an abuse precluded by Article 102 TFEU[21] [22]. Moreover, as suggested by Kerber[23], such a refusal to provide access to data might also, in certain circumstances, amount to an abuse of economic dependence[24].

This is supported by numerous recent reports underlining the need for a new competition law framework in light of the digital economy's characteristics[25]. Indeed, traditional competition law, as applied to "brick and mortar" industries, might not be appropriate to address competitive issues in the digital economy. This is because the digital economy is characterised by extreme returns to scale, network externalities – the more users a technology has, the more its usefulness increases for each user –, and the prominent role of data – being able to use data to develop or

[18] Barbero et al. (2018), pp. 92-93.

[19] Graef et al. (2018), pp. 10-11. See also Miller and Tucker (2014).

[20] CFI, 17 September 2007, T-201/04, *Microsoft I*; ECJ, 29 April 2004, C-418/01, *IMS Health*; ECJ, 26 November 1998, C-7/97, *Bronner*; ECJ, 6 April 1995, joined cases C-241/91 and C-242/91, *Magill*.

[21] Treaty on the Functioning of the European Union, OJ C 326/47, 26 October 2012.

[22] Drexl (2016), p. 44. On the applicability of the Essential Facilities' doctrine to data, see: Drexl (2016); Graef (2016); Graef et al. (2015); Colangelo and Maggiolino (2017).

[23] Kerber (2018), p. 329. See also Tombal (2020).

[24] Gesetz gegen Wettbewerbsbeschränkungen, § 20 (Act against Restraints of Competition, adopted on 26 August 1998 and lastly amended on 19 January 2021. The official English translation of the GWB is available at http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0066); in France, see the Code de Commerce, article L. 420-2, al. 2 (Official translation available at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations); in Belgium, see the Code de droit économique, article IV.2/1.

[25] Crémer et al. (2019); Schweitzer et al. (2019); Schweitzer et al. (2018); Furman et al. (2019); Autorité de la concurrence and Bundeskartellamt (2016).

improve innovative products or services is a key competitive parameter[26]. These characteristics lead to strong economies of scope who benefit large incumbent digital players who have access to more (recent) data than their competitors, which makes it complicated to dislodge them[27]. In this context, providing access to a competitors' data as a remedy to an abuse of dominant position or to an abuse of economic dependence could therefore be seen as a pro-competitive solution entailing more data sharing.

Nevertheless, some of the data at hand could be personal data. Therefore, some tensions might emerge between competition law and personal data protection law[28]. Indeed, while competition law might require the sharing of personal data in order to stimulate innovation and to ensure a level playing field between incumbent data holders and undertakings who need access to these data, the GDPR subjects the processing of personal data to the principles of purpose limitation and data minimisation[29]. According to the purpose limitation principle, personal data can only be processed for specified, explicit and legitimate purposes, and cannot be further processed in a manner that is incompatible with those purposes. This means that data that has been collected for a specific purpose cannot be shared with third parties if this act of sharing does not fit within this initial purpose. According to the data minimisation principle, only the adequate, relevant and necessary personal data for the fulfilment of a specific purpose can be processed. This implies that, even if the act of data sharing complies with the purpose limitation principle, the categories and amount of data that can be shared should nevertheless be limited to what is necessary to meet this purpose. This outlines the importance of clearly defining the specific purpose of the data sharing remedy, as the GDPR prevents "over-sharing", i.e. sharing more data than what is relevant and necessary for the purpose of the processing.

To shed some light on how competition law and personal data protection law can be reconciled on this matter, this chapter will analyse how a competition authority's decision imposing to share personal data with a competitor can be compatible with the GDPR.

3. As a preliminary consideration, it should be outlined that one way to circumvent the application of the GDPR would be to anonymise the personal data before sharing it. However, this might reduce the value of

[26] Crémer et al. (2019), pp. 19-24.

[27] Crémer et al. (2019), pp. 3 and 24.

[28] On the articulation between competition law, personal data protection law and consumer law: see Graef et al. (2019).

[29] Art. 5.1.b) and c) of the GDPR. See also points 18 and 19 *infra*.

the dataset and, in any case, truly effective anonymisation[30] is difficult to achieve[31]. This is especially true in light of the constant development of *Big Data*[32] analytics, which increase the risk of re-identification of the data subjects. This failure to effectively anonymise personal data has been demonstrated several times in the literature[33], leading to the conclusion that what is often presented as anonymisation techniques are, in fact, merely pseudonymisation[34] techniques. Yet, pseudonymised data remain personal data covered by the GDPR, given that the data subject can still be re-identified.

In the vast majority of cases, the data will thus remain personal and the data sharing remedy will therefore have to comply with the rules of the GDPR. This requires, on the one hand, to have a lawful basis for the data sharing[35], and, on the other hand, to comply with the general principles of personal data protection[36]. Moreover, competition and data protection authorities will need to collaborate in order to define and implement this remedy.

I. Lawful basis for the data sharing

4. According to the principle of separate justification, a remedy imposing data sharing would require a lawful basis at two levels, namely at the level of the undertaking that transfers the data and at the level of the undertaking that will receive the data, and these two lawful bases do not

[30] The ISO 29100 standard defines anonymisation as the: "process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO 29100:2011, point 2.2, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en).

[31] Drexl (2018), p. 4. See also Graef et al. (2018), p. 6; and Wendehorst (2017), pp. 330-331.

[32] " 'Big data' is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software" (https://en.wikipedia.org/wiki/Big_data).

[33] Sweeney L. (1997); Rocher et al. (2019).

[34] "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Art. 4.5 of the GDPR).

[35] Article 6 of the GDPR.

[36] Article 5 of the GDPR.

need to be the same[37]. Therefore, this contribution will first address the potential lawful bases for the data holder before turning to the potential lawful bases for the data recipient.

A. Lawful basis for the data holder

5. Making personal data available to a third party as a consequence of a remedy imposed by a competition authority amounts to a new processing[38] for the data holder and is therefore in need of a lawful basis[39]. This raises a first preliminary question, namely whether a new separate lawful basis is necessary in order for the data sharing to be GDPR-compliant. Indeed, according to Article 6.4 and Recital 50 of the GDPR, a separate lawful basis is not necessary if the new purpose (*in casu* the data sharing as a remedy) is "compatible" with the initial purpose for which the data has been collected[40]. The question is thus whether imposing data sharing as a remedy could be considered as being compatible with the purpose of the initial data processing. To assess this compatibility, the following elements should be considered[41]:

- Any link between the initial purpose and the purpose of the intended further processing;
- The context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- The nature of the personal data;
- The consequences of the intended further processing for data subjects; and
- The existence of appropriate safeguards in both the original and intended further processing operations.

A key consideration here will be whether the data subjects could reasonably expect that the data holder might have to share the personal

[37] Wendehorst (2017), pp. 334-337.

[38] Processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Art. 4.2 of the GDPR).

[39] Wendehorst (2017), pp. 334-335.

[40] This is however contested by some authors, who argue that the final text of the GDPR fails to reflect the agreement that was reached during the negotiations (see Wendehorst (2017), pp. 335-336 and references cited in footnote 25 of that paper).

[41] Art. 6.4 and Recital 50 of the GDPR.

data it holds with another undertaking as a result of a competition law remedy. Can it be said that if a data subject provides its data to Facebook or Google, (s)he can reasonably expect that these firms might abuse their dominant position and that, as a consequence, they will have to share the personal data they hold with competitors? In conducting this assessment, the types of services that the competitors intend to offer and the potential safeguards that they would set in place, such as pseudonymisation mechanisms, should be considered. Moreover, this assessment of the compatibility of the purposes from a data protection perspective is interesting to compare with the assessment of the re-use purpose from a competition law perspective, as they might actually lead to contradictory findings. Indeed, from a data protection perspective, the purpose will more likely be considered as compatible if the service for which the recipient will use the data is similar to the service provided by the data holder. Conversely, if the recipient intends to use the data for another type of service, this might not be considered as a compatible purpose. In contrast, from a competition law perspective, the conditions to force a data holder to share its data with a recipient wishing to offer similar services should allegedly be harder to meet than the conditions to force a data holder to share its data with a recipient wishing to offer "new" types of services[42].

6. Concluding that the transfer is compatible with the initial purpose of processing would spare the necessity of identifying a separate lawful basis for the data holder and would thus facilitate the implementation of the data sharing remedy. If, on the other hand, the further processing deriving from the remedy imposing data sharing is deemed to be "incompatible" with the initial purpose for which the data has been collected – and this will likely often be the case –, this further processing can only be carried out if the data subjects have consented to it or if it is mandated by a legal obligation[43]. Indeed, only two of the six lawful bases listed in Article 6.1 of the GDPR can be relied upon to legitimise an incompatible further processing. This is the result of a compromise reached between the European Commission, the Working Party 29 (today the European Data Protection Board) and the European Parliament during the negotiations

[42] See, in this regard, the Essential Facilities Doctrine, according to which a refusal to provide the access to an essential facility will be considered as being an abuse of dominant position if the following exceptional circumstances are met: (i) the access to the facility is indispensable to compete on the downstream market; (ii) the refusal to grant access excludes all effective competition on the downstream market and (iii) prevents the introduction of a *new product/technological innovation*; and (iv) there is no objective justification for the refusal (emphasis added). See the case law and legal literature cited in footnotes 20 and 22.

[43] Art. 6.4 of the GDPR.

of the final text of the GDPR[44]. While the Commission only wanted to exclude the possibility to rely on the "legitimate interests" lawful basis[45] for incompatible further processing, the Working Party 29 and the European Parliament wanted to exclude the possibility to rely on any lawful basis at all because, by essence, such an incompatible further processing would be unlawful and therefore prohibited[46]. Indeed, according to the Working Party 29, "legalising an otherwise incompatible data processing activity simply by changing the terms of a contract with the data subject, or by identifying an additional legitimate interest of the controller, would go against the spirit of the purpose limitation principle and remove its substance"[47]. Yet, such a drastic position would have been highly problematic in the perspective of *Big Data* and *Open Data*. Accordingly, a compromise was reached, having in mind that the key concern of the GDPR is to provide control to the data subjects on what happens with "their" data. In order to avoid opacity towards incompatible further processing and to ensure transparency, it was thus decided that these processing could only be carried out if the data subjects had consented to them or if they were mandated by a legal obligation[48].

In light of the above, two lawful bases could potentially be used for the transfer of the personal data covered by the competition law remedy, namely consent and the necessary processing for the compliance with a legal obligation to which the data holder is subject[49].

1. Consent

7. The first possibility for the data holder would be to obtain the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision[50]. Indeed, obtaining a general consent *before* the decision will lack the specificity and explicitness required for the consent to be compliant with the GDPR[51]. The data holder will therefore have to seek the consent to share the data with one or several specific recipients identified in the competition authority's decision[52]. In this context, the data holder should

[44] Gaullier (2018), p. 51.
[45] Art. 6.1.f) of the GDPR
[46] Gaullier (2018), p. 51. See also Working Party 29 (2013), pp. 36-37.
[47] Working Party 29 (2013), p. 36.
[48] Gaullier (2018), p. 51.
[49] Arts. 6.1.a) and c) of the GDPR.
[50] Arts. 4.11 and 6.1.a) of the GDPR.
[51] Kathuria and Globocnik (2019), pp. 27-28.
[52] Kathuria and Globocnik (2019), p. 28.

request some basic information from the various data recipients (such as the purpose for which they will process the data or the types of data they will process[53]) in order to provide the data subjects with sufficient information allowing them to make a specific and informed choice about whether to consent to the transfer or not. However, it might be extremely complex and burdensome to do so in practice.

The French *GDF Suez*[54] case illustrates this point. The French *Autorité de la concurrence* found that GDF Suez had abused its dominant position in the market for natural gas and required GDF Suez to share certain customer information data with its competitors[55]. In order to avoid the burdensome collection of the consent of each and every data subject concerned by the remedy, the *Autorité*, after having consulted the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*), ordered GDF Suez to inform the data subjects about the sharing of their data with their competitors and to give them the possibility to opt-out from this transfer[56]. Given that, at the time, the Data Protection Directive[57] was still in force and that this legislation was silent about whether such an opt-out solution was admissible, this seemed like an appropriate way to balance the personal data protection and competition considerations[58].

However, now that the GDPR is in force, requiring the data subjects to opt-out of the transfer, rather than to opt-in to the transfer, would no longer be GDPR-compliant, as, according to Article 4.11 of the GDPR, the data subject has to explicitly consent to the transfer[59]. The necessity of an explicit consent has been confirmed by the European Court of Justice[60] and this makes it much more cumbersome for the data holder and will surely affect the efficiency in practice of the data sharing remedy if the data holder relies on consent as a lawful basis for the transfer.

---

[53] The data recipient could, for instance, produce a short form that would be filled in by the recipients and that would be presented to the data subjects when asking for their consent.

[54] Autorité de la concurrence, Decision n° 17-D-06 (GDF Suez), 21 March 2017, available on http://www.autoritedelaconcurrence.fr/pdf/avis/17d06.pdf.

[55] Graef (2016), pp. 271-272.

[56] Kathuria and Globocnik (2019), p. 28.

[57] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L 281/31.

[58] Kathuria and Globocnik (2019), p. 28. It should however be emphasised that according to some authors, consent under the Directive still required an (explicit) action from the data subject and couldn't be inferred from a lack of action (see Kosta (2015)).

[59] Kathuria and Globocnik (2019), p. 28.

[60] ECJ, 1 October 2019, C-673/17, *Planet 49*.

Indeed, it is very likely that there will be fewer data subjects that opt-in than data subjects that do not opt-out[61]. The intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent[62]. Additionally, relying on consent might also weaken this remedy as, according to Article 7.3 of the GDPR, the data subjects are free to withdraw their consent at any time.

2. Necessary for the compliance with a legal obligation to which the data holder is subject

8. The second possibility for the data holder would be to assume that the transfer is necessary for the compliance with a legal obligation to which he is subject[63]. The issue is whether a decision by a competition authority could qualify as such a legal obligation. Here, different views are expressed. While Graef indicates that a data sharing remedy imposed by a competition authority would amount to such a legal obligation[64], Kathuria and Globocnik argue, on the contrary, that a competition authority's decision will not qualify as a legal obligation for the data sharing, because this term presupposes the existence of an underlying generally applicable law[65].

Article 5.3 GDPR indeed provides that the basis for the processing shall be laid down in Union law or Member State law. However, the word "law" is not defined anywhere in the GDPR. In that regard, the interpretation, by the European Court of Human Rights, of the requirement of the legality of an interference with a fundamental right[66] should be reminded. The Court consistently holds that the term "law" must not be given a "formal interpretation", which would necessarily imply the existence of a written statute having a legislative value, but rather a "material interpretation"[67], which not only covers the written statutes, but all the legal rules in force[68]. Indeed, the European Court of Human Rights has, at the outset, recognised that in countries having a *Common Law* legal tradition, unwritten rules of law could be considered as satisfying the requirement of legality

[61] Kathuria and Globocnik (2019), pp. 28-29. See also Campbell et al. (2015).
[62] Kathuria and Globocnik (2019), p. 28.
[63] Art. 6.1.c) of the GDPR.
[64] Graef (2016), p. 319.
[65] Kathuria and Globocnik (2019), pp. 21-22.
[66] *In casu* article 8 of the European Convention on Human Rights (Right to respect for private and family life), in which personal data protection is rooted.
[67] Degrave (2014), p. 144.
[68] Ergec (2014), p. 232.

of interference in a fundamental right[69]. Importantly, the Court then also subsequently recognised a wider margin of manoeuvre for countries having a *Continental Law* legal tradition as to what should be incorporated under the term "law"[70]. In particular, the Court acknowledged that parliamentary proceedings, decisions, regulations or unwritten rules of law, such as case law decisions, could satisfy the requirement of legality[71].

Arguably, a similar interpretation could be given to the words "law" and "legal obligation" in the GDPR. This interpretation is supported by the fact that Recital 41 of the GDPR provides that "where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned".

However, Recital 41 also provides that, in accordance with the case-law of the European Court of Human Rights and the European Court of Justice, this "law" must be formulated in clear and precise terms, and be sufficiently predictable and accessible[72]. The requirement of predictability implies that anyone must be able to foresee, with a reasonable degree of certainty, the potential effects of this "law"[73]. This is where difficulties might emerge from a *Continental Law* perspective, as this would require for the case law on data sharing as a competition law remedy to be well-established, so that it has become clear and predictable. Yet, in practice, such case law is scarce and it might therefore be argued that the "law" is not sufficiently predictable at this point. Nevertheless, with time, such case law could develop more clearly and systematically, rendering it "predictable" and, as a consequence, a competition authority's decision imposing to provide access to data could qualify as a "legal obligation". As this is a key issue for the future, a clarification by the European Data Protection Board and the European Data Protection Supervisor on the matter would be highly welcomed.

In any case, in order to be GDPR-compliant, the data sharing remedy imposed by the competition authority will have to be specific enough. Indeed, Article 5.3 of the GDPR provides that the legal obligation should[74]

---

[69] ECtHR, *Sunday Times v. United Kingdom*, 26 April 1979, req. n° 6538/74, §§ 46-53.

[70] ECtHR, *Hüvig v. France*, 24 April 1990, req. n° 11105/84, § 28; and *Kruslin v. France*, 24 April 1990, req. n° 11801/85, § 29. See De Hert (2004), p. 716.

[71] De Hert (2004), p. 716.

[72] See also Ergec (2014), p. 232.

[73] Ergec (2014), p. 232.

[74] Art. 5.3 of the GDPR uses the word "may" but, in light of the decision of the European Court of Human Rights in the *Rotaru* (ECtHR, *Rotaru v. Romania*, 4 May 2000, req. n° 28341/95) and *Shimolovos* (ECtHR, *Shimovolos v. Russia*, 21 June 2011, req. n° 30194/09) cases, we argue that the appropriate word should be "should".

specify the purpose for which the data is shared (e.g. to remedy a specific competition issue), the undertakings with whom the data is shared, and the types of data and the data subjects concerned by the data sharing remedy. Moreover, Article 5.3 of the GDPR adds that this legal obligation should meet an objective of public interest (*in casu* ensuring a competitive environment that will benefit the consumers) and be proportionate to the legitimate aim pursued. In this regard, the competition authority must ensure that its decision does not disproportionally affect the data subjects' interests and rights.

B. Lawful basis for the data recipient

9. According to the principle of separate justification, while the data holder has to have a lawful basis to transfer the data towards the recipient, this recipient also needs his own specific lawful basis for the processing of the data that will be done once he has received the data covered by the data sharing remedy[75]. Similarly than for the data holder, this raises a first preliminary question, namely whether a new separate lawful basis is necessary in order for the data sharing to be GDPR-compliant. In this regard, the data recipient could attempt to demonstrate that it will re-use the data for scientific research[76] or statistical[77] purposes as, in those cases, the further processing is considered as compatible with the initial purpose of processing and no separate lawful basis is necessary[78]. In such cases, appropriate technical and organisational safeguards, such as pseudonymisation, would, however, have to be set[79]. As pointed out by Mayer-Schönberger and Padova (2016), this could notably be possible for some *Big Data* applications.

10. If the data recipient is not able to rely on the above-mentioned exemption for scientific research or statistical purposes, he will have to

[75] Wendehorst (2017), pp. 334-337.

[76] According to Recital 159 of the GDPR, scientific research purposes "should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research (…) [and] should also include studies conducted in the public interest in the area of public health".

[77] Statistical purposes mean "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that (…) the personal data are not used in support of measures or decisions regarding any particular natural person" (Recital 162 of the GDPR).

[78] Art. 5.1.b) and Recital 50 of the GDPR.

[79] Art. 89.1 of the GDPR.

rely on a new lawful basis of processing. However, we argue that, contrary to the data holder[80], he will have the ability to rely on any of the six lawful bases contained in Article 6.1 of the GDPR[81]. This is because the potential incompatibility of purposes will have been "purged" either by the consent or the legal obligation that has been used as a lawful basis for the transfer of the data from the holder to the recipient.

In practice, the data recipient will rely either on consent or on "legitimate interests" for the further processing. Indeed, contrary to the data holder, the recipient should not be able to argue that this further processing is necessary for the compliance with a legal obligation to which he is subject. This is because, while the competition authority's decision to impose a data sharing remedy could be considered as a legal obligation for the data holder that must comply with this decision[82], this decision does not impose any obligation on the data recipient to process the shared data. Therefore, the recipient cannot argue that he must necessarily process the data as a result of the competition authority's decision.

1. Consent

11. The first lawful basis for the data recipient could thus be the obtaining of the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision[83]. In this regard, the data recipient will have to be very specific about the purpose for which he will use this data, as the data subject's consent should be asked for a well-defined purpose and should not remain general[84]. However, and similarly than for the data holder, it might be extremely complex and burdensome to do so in practice and the intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent[85]. Additionally, relying on consent might also weaken this remedy as, according to Article 7.3 of the GDPR, the data subjects are free to withdraw their consent at any time.

[80] See *supra* point 6.

[81] Namely: (i) consent, (ii) processing necessary for the performance of a contract; (iii) processing necessary for compliance with a legal obligation; (iv) processing necessary in order to protect the vital interests; (v) processing necessary for the performance of a task carried out in the public interest; and (vi) processing necessary for legitimate interests.

[82] See *supra* point 8.

[83] Arts. 4.11 and 6.1.a) of the GDPR.

[84] Art. 6.1.a) and 8.2 of the GDPR.

[85] Kathuria and Globocnik (2019), p. 28.

2. Necessary for the purposes of the legitimate interests pursued by the data recipient

12. The other possibility for the data recipient would be to argue that the data processing is necessary for the purposes of the legitimate interests that he pursues, and that these interests are not overridden by the interests or fundamental rights and freedoms of the data subjects[86]. This requires to identify legitimate interests for the data recipient, to demonstrate that the data processing resulting from the data sharing remedy is necessary to fulfil these legitimate interests, and to strike a balance between the interests of the data recipient, on the one hand, and the interests of the data subjects, on the other hand.

For the data recipient, the legitimate interests of the access would be the opportunity to offer (privacy-oriented) alternative products or services to the consumers, to restore competition on the market where the data holder has committed an abuse, and to reduce the latter's competitive advantage[87]. Moreover, processing the data covered by the remedy would arguably be necessary for the data recipient in order to fulfil these legitimate interests, as, in principle, the competition authority will have ordered the data sharing precisely because there was no other remedy to achieve these interests in light of the competition law infringement committed by the data holder (e.g. the data sharing remedy is imposed because it is the only way to reduce the data holder's competitive advantage and to restore competition, and the recipient has to use this data if it wants to be able to offer alternative products or services).

The key question is therefore whether the data recipient's legitimate interests outweigh the data subjects' interests. At first glance, the data sharing deriving from the competition authority's decision might look like it will always risk affecting the data subjects' rights, as more undertakings will get access to their personal data, thus potentially reducing the data subjects' privacy. Moreover, it might also arguably increase the risks of de-anonymisation of other data[88]. Accordingly, there might be some cases where the data subjects will be worse off because of this data sharing. In such cases, the legitimate interests of the data recipient should not prevail over the data subjects' interests, and Article 6.1.f) GDPR should not be considered as a viable lawful basis.

[86] Art. 6.1.f).
[87] Kathuria and Globocnik (2019), p. 25.
[88] Kathuria and Globocnik (2019), pp. 26 and 32.

However, there are other cases where this data sharing might allow competitors to create privacy-oriented alternatives to existing services, which would benefit the data subjects in the long term. Indeed, the development of competitive alternatives is necessary to prevent data subjects from being "locked in" the services of the existing providers, as more switching possibilities would allow the data subjects to "penalise" more easily data controllers that (repeatedly) violate their privacy. To support this argument, the "About Data About Us" report should be mentioned[89]. It is the result of a collaboration in the United Kingdom between the Open Data Institute, Luminate, and the Royal Society for the encouragement of Arts, Manufactures and Commerce. These institutions explored, via focus groups and a workshop, how UK citizens feel about "their" data and about the (lack of) control and protection they experience[90]. The report outlines that people have much more awareness and understanding about these issues than what they are traditionally given credit for by politicians and in the press (where they are traditionally painted as naïve or ignorant), and that people do have clear expectations on how "their" data should be protected[91]. They desire more transparency, more control, more fairness and more compliance with personal data protection principles from the undertakings that process their data[92]. Therefore, if the data recipients were to offer more privacy-oriented alternatives than the data holder's services, the legitimate interests of the data recipients could prevail over the data subjects' interests – and might actually be aligned with these interests –, and accordingly the data could be shared on the basis of Article 6.1.f) GDPR.

In order to achieve the above-mentioned balancing exercise between the interests of the data recipient and those of the data subjects, the data recipient will need to be very specific about the use he will make of the shared data (e.g. which products or services he intends to offer thanks to the data, whether they are privacy-oriented or not, etc.), as this will allow to determine if this further processing would be harmful, or on the contrary beneficial, to the data subjects. Naturally, the data subjects will remain free to oppose to this processing on the basis of Article 21.1 of the GDPR, if they disagree with the outcome of the balance of interests.

89 Samson et al. (2019).
90 Samson et al. (2019), p. 3.
91 Samson et al. (2019), p. 39.
92 Samson et al. (2019), pp. 36-38.

C. Findings

13. In light of the above, it appears that the privileged option, in terms of the lawful basis to be used by the data holder, would be to assume that an obligation to share personal data imposed by a competition authority amounts to a legal obligation that the data holder must comply with. Nevertheless, this would require to assume that the case law on data sharing as a competition law remedy is clear and predictable, which might arguably not be the case so far in light of the scarcity of the said case law. However, with time, such case law could develop more clearly and systematically, rendering it "predictable". Moreover, it must be kept in mind that some authors consider that a competition authority's decision shall not qualify as a legal obligation in the sense of Article 5.1.c) of the GDPR[93]. As this is a key issue for the future, a clarification by the European Data Protection Board and the European Data Protection Supervisor on the matter would be highly welcome.

Alternatively, the data holder could use the data subject's freely given, specific, informed and unambiguous consent, obtained *after* the competition authority's decision, as lawful basis of the processing. Nevertheless, it might be extremely complex and burdensome to do so in practice and the intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent[94]. Additionally, relying on consent might also weaken the competition law remedy, as, according to Article 7.3 of the GDPR, the data subjects are free to withdraw their consent at any time.

14. The data recipient, on the other hand, could attempt to demonstrate that it will re-use the data for scientific research or statistical purposes as, in those cases, the further processing is considered as compatible with the initial purpose of processing and no separate lawful basis is necessary[95]. If this is not the case, he will have to rely on a new lawful basis of processing.

In practice, the data recipient will rely either on consent or on "legitimate interests" for the further processing. Much like for the data holder, consent will be extremely complex and burdensome to obtain in practice and the intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent[96]. The data recipient will

[93] Kathuria and Globocnik (2019), pp. 21-22.
[94] Kathuria and Globocnik (2019), p. 28.
[95] Art. 5.1.b) and Recital 50 of the GDPR.
[96] Kathuria and Globocnik (2019), p. 28.

therefore likely attempt to rely on "legitimate interests", but the availability of this lawful basis will be function of the specific circumstances of the cases. Indeed, although there might be some cases where Article 6.1.f) GDPR will not be considered as a lawful basis, there might be some other cases where this further processing might allow competitors to create privacy-oriented alternatives to existing services, which would benefit the data subjects in the long term. In order to make this assessment, the data recipient will need to be very specific about the use he will make of the shared data, as this will allow to determine if this further processing would be harmful, or on the contrary beneficial, to the data subjects. Naturally, the data subjects will remain free to oppose to this processing on the basis of Article 21.1 of the GDPR, if they disagree with the outcome of the balance of interests.

15. It thus derives from this analysis that the effectivity of a competition remedy imposing data sharing might, in fact, be highly uncertain. Indeed, on the one hand, the data holder might arguably not be able to rely on the "legal obligation" lawful basis for the transfer of the data as long as the case law is not sufficiently clear and predictable. On the other hand, the data recipient might not always be able to rely on "legitimate interests" for his further processing, as there might be cases where his legitimate interests should not prevail over the data subjects' interests.

Therefore, the effectivity of a competition remedy imposing data sharing might ultimately depend on the data subjects' consent. While data subjects might not see the added-value of consenting to the processing of their personal data by a data recipient that would offer them a service that is similar to (or a copy of) the data holder's service, they might have more incentives to consent to the processing of their personal data by a data recipient that would offer them a "new" type of service or an alternative service that interoperates with the data holder's service[97]. Here, the objectives of data protection law are aligned with the objectives of competition law, as competition authorities will be more reluctant to force a data holder to share its data with a recipient wishing to offer similar services than to force a data holder to share its data with a recipient wishing to offer "new" types of services.

[97] On the necessity to go further than data portability and the necessity to ensure interoperability between services, see Crémer et al. (2019), pp. 58-60.

II. Compliance with the general principles of personal data protection

16. In order for data sharing as a remedy to be compatible with the data protection rules, the data holder and the data recipient must not only rely on a lawful basis for the processing (respectively for the transfer and for the further processing of the data). They must also comply with the general principles of personal data protection.

17. First, both the data holder and the data recipient will have to inform the data subjects about the personal data processing deriving from this data sharing remedy, in a fair and transparent manner[98]. On the one hand, the data holder will have to inform the data subjects that it has been compelled by a competition authority to make some of the personal data concerning them available to a third party as a remedy to an abuse[99]. On the other hand, the data recipient will have to inform the data subjects about the further processing it will conduct thanks to the data covered by the remedy[100]. In this regard, the data recipient will notably have to inform the data subjects about the categories of personal data concerned, about the purposes of the processing for which the personal data are intended and about the period for which the personal data will be stored[101]. This information is key as it will allow the data subjects to express a free, specific, informed and unambiguous consent.

The data recipient will have to provide this information within a reasonable period after obtaining the personal data. This period should be determined by considering the specific circumstances in which the personal data are processed, and should, in any case, never be longer than one month[102]. Nevertheless, if these personal data are used by the data recipient to communicate with the data subjects, this information will have to be provided at the latest at the time of the first communication[103]. According to the Working Party 29[104], this does not preclude the one-month time limit mentioned above, and therefore the data recipient will have to provide the information at the time of the first communication

98 Arts. 5.1.a) and 12 to 14 of the GDPR.
99 Article 13 of the GDPR.
100 Article 14 of the GDPR.
101 Arts. 14.1.c) and d) and 14.2.a) of the GDPR.
102 Art. 14.3.a) of the GDPR.
103 Art. 14.3.b) of the GDPR.
104 Replaced by the "European Data Protection Board" since the entry into force of the GDPR on 25 May 2018.

(if it takes place less than one month after having obtained the data) or at the latest one month after having obtained the data[105].

However, there are situations where this information duty will not apply. On the one hand, it will not apply if the data subject already has the information[106]. A data recipient might thus be tempted to say that the data subjects have already been informed by the data holder. Nevertheless, this will rarely be the case because the data holder will have provided information about the *transfer* but not about the *further processing* done by the data recipient (the former might allegedly not even be aware of the concrete processing that will be accomplished by the latter). On the other hand, this information duty will not apply if the provision of such information proves impossible or would involve a disproportionate effort[107]. Here, it should be mentioned that it will not always be easy for the data recipient to identify all the data subjects concerned by the data sharing, as the shared data might be pseudonymised or aggregated personal data that cannot be immediately linked to well-identified data subjects. In this context, it can be questioned whether the recipient has a duty to make sure that the data holder will pass on the necessary contact details of the data subjects, as this would likely conflict with the data minimisation principle[108], because this would entail the sharing of more data than is necessary for the purpose of the processing[109]. If, in light of the minimisation principle, these details are not passed on, it might be impossible or disproportionate for the data recipient to inform the data subjects.

18. Second, both the data holder and the data recipient will have to comply with the purpose limitation principle, according to which the transfer by the data holder and the further processing by the data recipient should be limited to specified, explicit and legitimate purposes[110]. This outlines the importance of defining in advice, and ideally already in the competition authority's decision, for which specific purpose the data shall be shared (e.g. which products or services the data recipient intends to offer thanks to the shared data).

19. Third, the data holder and the data recipient will have to comply with the data minimisation principle, according to which only the

[105] Working Party 29 (2018), p. 16.
[106] Art. 14.5.a) of the GDPR.
[107] Art. 14.5.b) of the GDPR.
[108] Art. 5.1.c) of the GDPR.
[109] Wendehorst (2017), pp. 340-341.
[110] Art. 5.1.b) of the GDPR.

adequate, relevant and necessary data for the fulfilment of the specific purpose justifying the data sharing shall be transferred by the data holder and processed by the data recipient[111]. Once again, this outlines the importance of defining in advice, and ideally already in the competition authority's decision, the specific purpose of the processing, in order for the data sharing remedy to cover only the data that is necessary to fulfil it. In the same vein, the accuracy of the shared data should be ensured and it should be stored by the data recipient for no longer than is necessary for this specific purpose[112].

20. Fourth, the data holder and the data recipient will have to ensure that the data subjects' rights are given their fullest effect[113]. Accordingly, if a data holder receives, from a data subject, a valid request for rectification or erasure[114] of some of the personal data covered by the data sharing remedy, it will have to notify it to the data recipient so that the data is also rectified or erased in the latter's dataset as well[115].

21. Finally, the data holder and the data recipient will have to implement appropriate technical and organisational measures in order to ensure the security of the data during the transfer and during the further processing[116], and they will have to document how the implementation of the data sharing remedy complies with all of the above-mentioned principles, in light of the accountability principle[117].

III. Need for competition and data protection authorities to collaborate

22. It stems from the above analysis that, while some tensions might emerge between competition law and personal data protection law, they are not incompatible, and they can be reconciled by making a competition law duty to share data compliant with data protection principles. Yet, this is no easy task and it might be quite complex in certain specific

[111] Art. 5.1.c) of the GDPR.
[112] Art. 5.1.d) and e) of the GDPR
[113] Arts. 15 to 22 of the GDPR.
[114] Arts. 16 and 17 of the GDPR.
[115] Art. 19 of the GDPR.
[116] Art. 5.1.f) and 32 of the GDPR.
[117] Art. 5.2 of the GDPR

situations. In practice, this implies the need for competition and data protection authorities to collaborate on this matter. Indeed, a competition authority might not be the best suited to handle these personal data protection aspects alone[118]. Accordingly, the competition authorities should solicit the help of data protection authorities in defining the appropriate data sharing remedy, as the French *Autorité de la concurrence* has done in the *GDF Suez* case[119], where it consulted the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*). The data protection authority could then be put in charge of supervising the correct implementation of the remedy from a personal data protection perspective. This might however create practical challenges, such as overlaps between the powers of the competition and personal data protection authorities, and more research is needed on how these can be overcome. Finally, this implies the need to interpret data protection law and competition law provisions in a coherent manner, in order to minimise conflicts and to maximise complementarity between these regimes[120].

Conclusion

23. The objective of this chapter was to analyse how a competition authority's decision imposing to share personal data with a competitor can be compatible with the GDPR. This requires, on the one hand, having a lawful basis at two levels – namely a lawful basis for the *transfer* by the data holder and a lawful basis for the *re-use* by the data recipient –, and, on the other hand, to comply with the general principles of personal data protection (duty to inform the data subject, purpose limitation, minimisation and accountability principles, etc.). Moreover, competition and

[118] This can be illustrated by the fact that the *Bundeskartellamt*'s (the German competition authority) decision in the *Facebook* case (case n°B6-22/16, 6 February 2019), where it prohibited Facebook from combining user data from different sources, was suspended by the Higher Regional Court of Düsseldorf (case n° VI-Kart 1/19 (V), 26 August 2019) which expressed serious doubts regarding the legality of the authority's decision, notably for relying on competition law to tackle what appeared to be a personal data protection issue. However, this decision of the Dusseldorf Higher Regional Court has been overturned by the *Bundesgerichtshof* (German Federal Court of Justice), which confirmed the *Bundeskartellamt's* approach (case n° 080/2020, 23 June 2020, KVR 69/19).

[119] Autorité de la concurrence, Decision n° 17-D-06 (GDF Suez), 21 March 2017, available at http://www.autoritedelaconcurrence.fr/pdf/avis/17d06.pdf.

[120] Graef et al. (2019), p. 31.

data protection authorities will need to collaborate in order to define and implement this remedy.

The privileged option, in terms of the lawful basis to be used by the data holder for the transfer of the data towards the recipient, would be to assume that an obligation to share personal data imposed by a competition authority amounts to a "legal obligation" that the data holder must comply with. Nevertheless, this would require to assume that the case law on data sharing as a competition law remedy is clear and predictable, which might arguably not be the case so far in light of the scarcity of the said case law. However, with time, such case law could develop more clearly and systematically, rendering it "predictable". As this is a key issue for the future, a clarification by the European Data Protection Board and the European Data Protection Supervisor on the matter would be highly welcome. Alternatively, the data holder could use the data subject's freely given, specific, informed and unambiguous consent, obtained *after* the competition authority's decision, as lawful basis of the processing. Nevertheless, it might be extremely complex and burdensome to do so in practice and the intended remedy's goal might therefore not be reached if only a few of the data subjects effectively consent[121].

The data recipient, on the other hand, could attempt to demonstrate that it will re-use the data for scientific research or statistical purposes[122] as, in those cases, the further processing is considered as compatible with the initial purpose of processing and no separate lawful basis is necessary[123]. If this is not the case, he will have to rely on a new lawful basis for the further processing. In practice, the data recipient will rely either on consent or on "legitimate interests". Much like for the data holder, consent will however be extremely complex and burdensome to obtain in practice. The data recipient will therefore likely attempt to rely on "legitimate interests", but the availability of this lawful basis will be function of the specific circumstances of the cases.

In light of the above, the effectivity of a competition remedy imposing data sharing might, in fact, be highly uncertain. Indeed, on the one hand, the data holder might arguably not be able to rely on the "legal obligation" lawful basis for the transfer of the data as long as the case law is not sufficiently clear and predictable. On the other hand, the data recipient might not always be able to rely on "legitimate interests" for his further processing, as there might be cases where his legitimate interests should not prevail over the data subjects' interests. Therefore, the effectivity of a

[121] Kathuria and Globocnik (2019), p. 28.

[122] For a definition of "scientific research" and "statistical purposes", see footnotes 76 and 77.

[123] Art. 5.1.b) and Recital 50 of the GDPR.

competition remedy imposing data sharing might ultimately depend on the data subjects' consent. Such a finding casts doubts on the argument according to which *ex post* competition law intervention would be able to efficiently tackle market failures deriving from insufficient data access. This finding also justifies the need for a discussion on alternative solutions than resorting to competition law, such as the potential creation of *ex ante* regulation providing for data access in certain specific cases. In fact, such discussions on *ex ante* regulation have recently become much more concrete, following the adoption, by the European Commission, of its proposals for a Data Governance Act[124] and for a Digital Markets Act[125].

References

[1] Autorité de la concurrence and Bundeskartellamt (2016) "Competition Law and Data", http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

[2] Barbero M., Cocoru D., Graux H., Hillebrand A., Linz F., Osimo D., Siede A, Wauters P. (2018) Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 25 April 2018, available at https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-reusability-and -access-data-and.

[3] Campbell J., Goldfarb A., Tucker C. (2015) "Privacy regulation and market structure", *Journal of Economics & Management Strategy*, 24(1), pp. 47-73.

[4] Colangelo G., Borgogno O. (2018) "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", *Stanford-Vienna European Union Law Working Paper No. 35*, available at https://law.stanford.edu/publications/no-35-data-innovation-and-transatlantic-competition-in-finance-the-case-of-the-access-to-account-rule/.

[5] Colangelo C., Maggiolino M. (2017) "Big data as misleading facilities", *European Competition Journal*, Issue 13, Vol. 2-3, pp. 249-281.

[124] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final.

[125] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final.

[6] Crémer J., de Montjoye Y.-A., Schweitzer H. (2019) "Competition Policy for the digital era – Final report", *Report by the special advisers of Commissioner Vestager*, available at http://ec.europa.eu/competition/publications/reports/ kd0419345enn.pdf.

[7] De Hert P. (2004) "Artikel 8. Recht op privacy", in Handboek EVRM, Deel 2. Artikelsgewijze commentaar, Vande Lanotte J., Haeck Y. (dir.), Vol. 1, Antwerp, Intersentia, pp. 705-788.

[8] Degrave E. (2014), L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, Collection du CRIDS, Bruxelles, Larcier.

[9] Drexl J. (2018) "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", Max Planck Institute for Innovation & Competition Research Paper No. 18-23, available at: https://ssrn.com/abstract=3274519.

[10] Drexl J. (2016) Designing Competitive Markets for Industrial Data - Between Propertisation and Access (October 31, 2016), Max Planck Institute for Innovation & Competition Research Paper No. 16-13, available at SSRN: https://ssrn.com/abstract=2862975.

[11] Ergec. R. (2014) Protection européenne et internationale des droits de l'homme, 3e édition, Bruxelles, Larcier.

[12] European Commission (2017) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Building a European Data Economy", Brussels, 10 January 2017, COM(2017) 9 final.

[13] European Commission (2018a) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", 25 April 2018, COM(2018) 232 final.

[14] European Commission (2018b) Commission Staff Working Document, "Guidance on sharing private sector data in the European data economy", accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", 25 April 2018, SWD(2018) 125 final.

[15] Furman J., Coyle D., Fletcher A., Marsden P., McAuley D. (2019) "Unlocking Competition", *Report of the Digital Competition Expert Panel for the British Chancellor of the Exchequer and Secretary of State for Business, Energy and Industrial Strategy*, available at https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel.

[16] Gaullier F. (2018) "Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau", *Communication commerce électronique*, 2018/4, pp. 45-52.

[17] Graef I., Tombal T., de Streel A. (2019) "Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law", *TILEC Discussion Paper No. DP 2019-024*, available at https://ssrn.com/abstract=3494212.

[18] Graef I., Gellert R., Husovec M. (2018) "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *TILEC Discussion Paper No. 2018-028*, available at http://ssrn.com/abstract=3256189.

[19] Graef I. (2016) *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Alphen aan den Rijn, Kluwer.

[20] Graef I., Wahyuningtyas S. & Valcke P. (2015) "Assessing data access issues in online platforms", *Telecommunications Policy*, Vol. 39, pp. 375-387.

[21] Haucap J. (2018) "A German approach to antitrust for digital platforms", in *Digital Platforms and Concentration, Second annual antitrust and competition conference*, pp. 8-13, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf.

[22] Information Commissioner's Office (2019) "Data sharing code of practice – Draft code for consultation", available at https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf.

[23] Kathuria V., Globocnik J. (2019) "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", Max Planck Institute for Innovation and Competition Research Paper No. 19-04, available at https://ssrn.com/abstract=3337524.

[24] Kerber W. (2018) "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data", *JIPITEC*, 9 (2018), pp. 310-331.

[25] Kosta E. (2015) "Construing the Meaning of 'Opt-Out': An Analysis of the European, U.K. and German Data Protection Legislation", *European Data Protection Law Review*, 2015, Vol. 1, pp. 16-31.

[26] Mayer-Schönberger V., Padova Y. (2016) "Regime change? Enabling Big Data through Europe's new Data Protection Regulation", *Columbia Science & Technology Law Review*, Vol. XVII 2016, pp. 315-335.

[27] Miller A., Tucker C. (2014) "Health information exchange, system size and information silos", *Journal of Health Economics*, 33(2), pp. 28-42.

[28] Muralidhar K., Sarathy R., Li H. (2014) "'To Share or Not to Share. That is Not the Question' - A Privacy Preserving Procedure for Sharing Linked Data", available at https://ssrn.com/abstract=2462152.

[29] Rocher L., Hendrickx J., de Montjoye Y.-A. (2019) "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, Vol. 10, n° 3069, available at https://www.nature.com/articles/s41467-019-10933-3.

[30] Samson R., Gibbon K., Scott A. (2019) "About data about us", available at https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf.

[31] Schweitzer H., Schalbruch M., Wambach A., Kirchhoff W., Langeheine D., Schneider J.-P., Schnitzer M., Seeliger D., Wagner G., Durz H., Heider M., Mohrs F. (2019) "A New Competition Framework for the Digital Economy", *Report by the Commission "Competition Law 4.0" for the German Federal Ministry for Economic Affairs and Energy*, available at https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competition-framework.pdf?__blob=publicationFile&v=2.

[32] Schweitzer H., Haucap J., Kerber W., Welker R. (2018) "Modernising the law on abuse of market power", *Report for the German Federal Ministry for Economic Affairs and Energy*, available at https://www.bmwi.de/Redaktion/DE/Downloads/Studien.

[33] Sweeney L., "Weaving Technology and Policy Together to Maintain Confidentiality", *Journal of Law, Medicine & Ethics*, 1997, Vol. 25, Issues 2 & 3, pp. 98-110.

[34] Tombal T. (2020) "Economic dependence and data access", *IIC*, Issue 51(1), 2020, pp. 70-98.

[35] Vezzoso S. (2018) "Fintech, Access to Data, and the Role of Competition Policy", available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106594.

[36] Wendehorst C. (2017) "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy', in *Trading Data in the Digital Economy: Legal Concepts and Tools*, Lohsse S., Schulze R., Staudenmayer D. (eds.), Baden Baden, Nomos - Hart Publishing, pp. 327-355.

[37] Working Party 29 (2018) "Guidelines on transparency under Regulation 2016/679", WP 260 rev.01, 11 April 2018, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[38] Working Party 29 (2013) "Opinion 03/2013 on purpose limitation", WP 203, 2 April 2013, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.