CiTiP Working Paper Series

White Paper on the Data Act Proposal

Edited by

Charlotte Ducuing
Thomas Margoni
Luca Schirru

CiTiP Working Paper 2022

KU Leuven Centre for IT & IP Law - imec

26 October 2022

White Paper on the Data Act

Table of Contents

party, thereby disincentivising third parties to engage. The reading of both Article 5(3)[84] and (5)[85] however suggests that the European Commission may have envisaged this option, while attempting to regulate the possible detrimental consequences on the third party. The opposite situation – where the data holder would not sort data out and would share all data generated by the use of the product or related service to the chosen third party – seems much less likely. This being, the Data Act proposal is actually not clear on which data the chosen third party is entitled to. In any case, it is likely to require lengthy negotiations between the data holder and chosen third party.[86]

2.3 Main conclusions and recommendations

The ambition of the European Commission to protect users against harmful use of data by data holders (defensive facet of data control) in laudable. However, there is room for improvement, by extending the effect of the limitations downstream the data transactions initiated by data holders. The notion of 'use' should be clarified, in particular in contrast to 'processing'. While the first sentence of Article 4(6) raises many questions, the legislator should clarify the rationale, or else a sound alternative rule should be substituted, such as a simple deletion,[87] the right for the user to request a contractual agreement on the use of data[88] and/or a list of legal bases for the processing of data by the data holder inspired by Article 6 of the GDPR.

Concerning the positive facet of data control, it is only logical that the data portability right is not subject to exhaustion, which should be clarified expressly. Besides, it may be advisable that the Data Act further regulates how to align data 'demand' and 'offer' in a certain data portability instance. Two suggestions can be made at this point. First, transparency obligations should not only be targeted at users but also at chosen third parties, possibly in the form of a right for the chosen third party to request a number of relevant further information to the data holder. Second, we posit the hypothesis that the alignment of data 'offer' and 'demand' in a given instance could constitute an activity for data intermediaries to facilitate the implementation of the data portability mechanism, as flexible and neutral market facilitators (on the role that data intermediaries could play, see section 17.5 of this White Paper).

3 The broadening of the right to data portability for IoT products: Who does the Act actually empower? – Daniela Spajic[89] and Teodora Lalova-Spinks[90]

[84] Article 5(3) reads as follows: 'The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.'

[85] Article 5(5) reads as follows: 'The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.'

[86] This was the warning raised by Kerber (n 81), sec 4.

[87] Preferred option according to Drexl and others (n 74) para 54.

[88] This is the 'second best' suggestion by Drexl and others (n 74) para 53.

[89] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[90] Clinical Pharmacology and Pharmacotherapy, Department of Pharmaceutical and Pharmacological Sciences, KU Leuven, Belgium. Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium. The authors have contributed equally to this work.

In light of the European Commission goal to create a data-agile economy, the empowerment of data subjects is currently at the centre of new EU policy initiatives.[91] The notion of empowerment is often equated with the strengthening of control over one's own personal data. It typically pertains to individuals and their empowerment through tools such as consent and the data subjects' rights. Especially the right to data portability enshrined in Article 20 GDPR is increasingly promoted as an essential tool, perhaps even as the main tool, to 'further strengthen' control of data subjects.[92] Yet, the Data Act proposal[93] introduces a substantial shift in the discourse about the data portability right and individual empowerment.

3.1 The Data Portability Right: Version 1.0, 2.0, 3.0, …

The GDPR was the first EU regulation to introduce a right to data portability. Pursuant to Article 20 GDPR, data subjects have the right to receive personal data concerning them and to transmit those data to another controller. The scope of the right, however, is fairly limited: first, the right can only be exercised where the processing of personal data is based on consent or contract and carried out by automated means.[94] Second, it applies only to personal data that was provided by the concerned data subject. Third, the transmission from one controller to another must be technically feasible.[95]

Despite its limited field of application, data portability as a tool is considered to be a key enabler to foster data sharing and to advance the data economy.[96] Therefore, it is not a surprise that the Data Act aims to broaden its scope in order to enable the re-use of data in a larger set of contexts.

3.1.1 Data portability in the Data Act

Put in concrete terms, the Data Act 'enhances' the data portability right for IoT products in the following ways:

1) the proposal extends the right to data portability from natural to legal persons;

2) the legal basis for the original processing of personal data is no longer limited to consent or contract but applicable to data processing based on any legal basis;

3) the right applies to the use of personal and non-personal data, as the applicable provision refers to any 'data generated by the use of a product or a related service';[97]

[91] Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final (Communication 'A European Strategy for Data').
[92] Ibid 10, 20.
[93] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM/2022/68 final (Data Act proposal).
[94] Regulation (EU) 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/EC [2016] OJ L 119/1 (GDPR), art 20(1)(a-b).
[95] GDPR, art 20(2).
[96] Communication 'A European Strategy for Data', 20-21.
[97] Data Act proposal, art 4(1).

4) the Data Act proposal explicitly specifies that the right applies to both 'actively provided' data, as well as 'passively observed' data (Recital 31 DA) [98] and finally;

5) the proposal mandates and ensures the technical feasibility of third-party access for all types of data (personal and non-personal),[99] thus going beyond the technical obligations prescribed in Article 20 GDPR (only for personal data).

Although the Data Act is the proposal that imposes the most significant changes to the right to data portability, the recently published proposal for a European Health Data Space Regulation (EHDS)[100] and the Data Governance Act[101] deserve mention as all three frameworks complement each other.

3.1.2 Data portability in the European Health Data Space

It is important to note that the recently published proposal for an EHDS broadens the scope of the right to data portability for the health sector yet again, thereby creating a sort of a third version of the concept. The proposal aims to ensure that 'data subjects can transmit their electronic health data, including inferred data, irrespective of the legal basis for the processing of the electronic health data'.[102] Unlike the Data Act proposal, EHDS' provisions afford the right to portability only to natural persons. But, same as the Data Act proposal, the right applies to both personal and non-personal data, as the EHDS introduces the notion of 'electronic health data' encompassing both personal and non-personal (electronic health) data.[103] Additionally, whilst the Data Act excludes 'inferred' or 'derived' data from its scope of application,[104] the EHDS includes 'inferred' and 'derived' data (including data obtained during a medical examination) as well as 'observed' and recorded data by automatic means into the scope of the right to data portability.[105] The Article 29 Working Party provided some clarification on these notions.[106] However, it remains unclear how the terms 'inferred', 'derived', and 'observed' data (used in the EHDS proposal) relate to the concepts of 'actively provided' and 'passively observed' data (under the Data Act proposal), as the Data Act proposal does not define the latter (on the lack of clarity of these notions, see also sec. 15.3 of this White Paper).

3.1.3 What about the Data Governance Act?

With a view to the DGA, data portability is expected to be one of the key enablers of altruistic data sharing and the re-use of personal data for scientific research purposes.[107] Notably, the right to data portability is not embedded in the DGA as such. Rather, the European data altruism consent form builds on this right since it should foster data portability 'where the data to be made available is not

[98] Ibid, rec 31.
[99] Ibid.
[100] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM/2022/197 final (EHDS proposal).
[101] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA).
[102] EHDS proposal, rec 12.
[103] Ibid 2(2)(a-c).
[104] Data Act proposal, rec 14.
[105] EHDS proposal, rec 5.
[106] Article 29 Working Party, 'Guidelines on the right to data portability under Regulation 2016/679' WP242 rev.01, 10.
[107] Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 38 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022.

held by the individual'.[108] For the empowerment of individuals, the DGA foresees the help of data intermediaries in supporting them with regard to the enforcement of their rights related to their personal data.[109]

3.2 Questioning the data portability new clothes

On the surface, the new 'enhanced' versions of the right to data portability appear to serve the goal of individual empowerment by remedying the limitations enshrined in the GDPR. However, a careful critical discussion of the broadened scope(s) of the right appears highly necessary to ensure that the individuals who will be empowered with the mechanisms are indeed, the individuals. For this section, we focus on highlighting several key uncertainties created through the broadening of the scope under the Data Act proposal.

3.2.1 Quid individual empowerment?

While broadening the scope of the data portability right may be generally welcome, it raises issues regarding the notions of individual empowerment and data control. Both notions were in the GDPR firmly linked to the personal data protection of data subjects, whereas the Data Act suggests extending data subjects' rights to legal persons. More specifically, the Data Act proposal moves away from the legal terminology introduced by the GDPR and establishes instead the notion of 'user', which refers to a 'natural or legal person that owns, rents or leases a product or receives a service'.[110] Users are afforded a right to access and use data generated by the use of products or related services [111] that could be perceived as a broadened right to data portability which commercial businesses could exercise.[112] This can be concluded based on a combined reading of the explanatory memorandum, the Impact assessment report that accompanies the Data Act proposal, and relevant recitals in the Data Act proposal (for example, Recital 31), even if it is not explicitly named as such in the law.

The opening of the data portability right to legal persons under the Data Act needs to be carefully examined. The Data Act proposal does establish safeguards against potential misuse of the portability right by legal persons, namely by stating that

> [w]here the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.[113]

However, would this be sufficient to ensure that no misuse occurs? Moreover, the reasoning of focusing on 'user' empowerment (in contrast to individual empowerment) is not made clear in the

[108] Commission, 'Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)' 8 COM(2020) 767 final, Explanatory memorandum.
[109] DGA, rec 30.
[110] Data Act proposal, art 2(5).
[111] Ibid, art 4.
[112] EDPB, EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 10 (2022).
[113] Data Act proposal, art 4(5).

Data Act proposal and its accompanying documents, especially as regards to the empowerment of legal persons over the use and portability of data subjects' personal data.

3.2.2 Data portability for personal and non-personal data

Furthermore, the broadening of the data portability right and its application irrespective of the legal ground on which the data processing is initially based, raises questions as regards to how the Data Act proposal has to be read or applied in conjunction with the GDPR. Regarding data portability, the Data Act gives users a right to share data (meaning in general terms any personal or non-personal data) with third parties irrespective of the legal ground based on which the processing of personal data takes place.[114] However, the enforcement of the data portability right by individuals under the GDPR is limited, so that only personal data can be ported when the data processing activity is based on consent and contract. Hence, there is a clear tension between Article 20 GDPR and Article 5 Data Act proposal regarding the scope of application, creating legal uncertainty on the porting or sharing of personal data requested by data subjects. This tension leads to the question as regards to the application of the Data Act proposal vis-à-vis the GDPR: should the Data Act proposal be applied as 'lex specialis'? The Data Act proposal appears to speak against such a view, as Article 1(3) Data Act proposal refers to Article 20 GDPR and states that the Data Act proposal 'shall complement the right of data portability under Article 20' GDPR where the personal data of users who are data subjects are concerned.[115] Consequently, if Article 20 GDPR is the relevant provision to be relied upon for the porting of personal data, then the provisions of the GDPR will collide with the Data Act proposal due to the limited scope of the data portability right under the GDPR.

3.3 Conclusion

With the entry into force of the Data Act proposal and the EHDS, we will have three different versions of the data portability right at our disposal. However, the rights differ not only in terms of scope but also by the terminology employed to describe them and enshrine them under the law. It remains to be explored how the three rights would apply in practice and, even more so, how the technical interoperability thereof will be guaranteed.

4 Chapter III – Making data available under FRAND terms – Charlotte Ducuing[116] and Luca Schirru[117]

4.1 FRAND Terms in the Data Act Proposal

'FRAND terms' stands for Fair, Reasonable and Non-Discriminatory terms. The content, and even the words, of what constitutes 'fair', 'reasonable' and 'non-discriminatory' may vary according to the regulation and/or sector under analysis.[118] Under the Data Act proposal,[119] specifically its Chapter III,

[114] Ibid, art 5.
[115] See also Data Act proposal, art 5(7), and EDPB-EDPS (n 113) 9.
[116] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[117] Postdoctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[118] On this, see in particular the analysis in Mathew Heim and Igor Nikolic, 'A FRAND Regime for Dominant Digital Platforms' (2019) 10 (1) JIPITEC <https://www.jipitec.eu/issues/jipitec-10-1-2019/4883> accessed 18 October 2022.
[119] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM/2022/68 final (Data Act proposal), arts 8 and 9.