The right to data portability: A holistic analysis of GDPR, DMA and the Data Act Proposal

Barbara Lazarotto[1]

Abstract

The right to data portability is a relatively new legal right introduced and enshrined by the General Data Protection Regulation with the objective of empowering data subjects to exercise agency over their data and how data controllers interact and safeguard the personal data entrusted to them. This right gives data subjects the right to obtain a copy of their personal data and to transfer such personal data directly from one data controller to another. Most recently, the Digital Markets Act and the Data Act Proposal have also introduced tertiary legal provisions building on the right to data portability, therefore adding a previously unforeseen nuance to it. However, due to many factors – such as the lack of proper regulation, presence of adequate technical capability, and data protection deadlocks – the right to data portability has found little or no practical application. Due to this innocuousness, data subjects keen on exercising their right to data portability are left in a grey zone, a position that consequently benefits data controllers that hold on to personal data that otherwise could be ported. In this context, this paper explores the current landscape of the right to data portability, with an examination of possible complementarities and conflicts between the General Data Protection Regulation, the Data Markets Act and the Data Act Proposal. This analysis will take into consideration the underlying objectives of these three Regulations, not only with the purpose of proceeding with a comparative analysis of the contours of the right to data portability under the aegis of these Regulations but to advance with a holistic analysis of the tangible application of the right and how these regulations might permit or hinder this application for the benefit of data subjects.

I. Introduction

The digital economy has been the centre of the European Data Strategy, due to data's potential to benefit businesses, researchers and public administration. Online platforms focused on the functioning of digital market are at the core of these discussions, since they have a special position in the digital information market[2], their practices established on the hyperfocus of promoting digital markets and exploitation of the personal as well as non-personal data of their consumers are often considered to be predatory and anti-competitive. As a result of the vast and unbridled data collection and processing activities undertaken by such market players, data-driven companies dominate online markets, diminish competition and hinder the accessibility and control which data subjects are awarded over their data through Regulations such as the GDPR.

---

1 Barbara Lazarotto is a PhD Researcher at the Vrije Universiteit Brussel and a Marie-Sklodowska Curie Action Fellow, she receives funding by the EU project "Legality Attentive Data Scientists", GA: 956562.

2 European Commission found in the context of the Google AdSense case that Google had a market share of generally over 90% in 2016 the market for general search in all Member States. in its investigation of Facebook, the German Federal Cartel Office found that Facebook had a market share in the market for social networks of over 95%. At Jan Kraemer, 'Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations', SSRN Scholarly Paper (Rochester, NY, 25 November 2020), https://papers.ssrn.com/abstract=3742771.

The sharing of data is considered to be a potential solution for ending such data monopolies, however, several barriers prevent an optimal sharing and transfer of data, such as a lack of incentives for data holders, legal uncertainties about the rights and obligations in relation to data owing to broad legislative provisions, absence of universal standards for semantic and technical interoperability. As an answer to this situation, the right to data portability was right introduced by the EU General Data Protection Regulation, which has as one of its main objectives the empowering of data subjects with more control over their data and, ultimately changing the market landscape from being data holder centric towards more consumer and consumer rights centric practices. This right to data portability gives the data subjects the right to obtain a copy of their personal data and to request the transfer of such personal data directly from one controller to another. Most recently, the Digital Markets Act and the Data Act Proposal also have touched on the right to data portability, adding new nuances to it, focusing on gatekeepers and access to data from the internet of things (IoT) and suppliers of related services respectively.

The aim of this article is to explore the current landscape of the right to data portability, with an examination of possible complementarities and conflicts between the General Data Protection Regulation, Data Markets Act and Data Act Proposal. Taking into consideration the underlying objectives of these three Regulations, not only with the purpose of proceeding with a comparative analysis of the right to data portability but to advance with a holistic analysis of the tangible application of the right and how these regulations might permit or hinder this application for the benefit of data subjects.

In this context, this article is structured as follows: Following this Introductory Section (Section I), Section II will outline the main aspects of the right to data portability in the three regulations separately, exploring its rationale, scope, objectives, and limitations through a text-based analysis of the GDPR, Data Markets Act and Data Act Legislative Proposal. Addressing the multiple interpretations of the texts; Further Section III will focus on a holistic analysis of the right to data portability, pondering how the right as it figures in these three regulations may intersect and how they differentiate, and how these similarities and differences may impact its application by individuals and consequently on the market. At last, the study is concluded on Section IV with a summary of the analysis and closing remarks.

II. Overview of the right to data portability in the three Regulations

This section focuses on the outline of the right to data portability as it figures in the three Regulations in chronological order, namely- (1) The analysis initiated by the GDPR which is already approved and entered into force in 2018; (2) the Data Markets Act, which has entered into force on 1 November 2022 and applies from 2 May 2023, and lastly; (3) the Data Act, which is still undergoing legislative procedure at the time of the writing of this study.

a) The Legal Debut of The Right to Data Portability: The General Data Protection Regulation

The General Data Protection Regulation (GDPR) was a paradigm shift regulation that entered into force on May 25, 2018, introducing a series of new rights to empower data

subjects, with the objective of giving them more control over their personal data[3] while encouraging its flow within the European Union.[4] [5] The GDPR introduced *The Right To Data Portability* in Article 20,[6] a novelty in the EU data protection framework,[7] with the aim of strengthening individuals' ability to exercise self-determination over their data while facilitating competition among data controllers through the sharing of data.

Since the GDPR is dedicated to protecting natural persons in relation to the processing of their personal data, Article 20 GDPR only applies to transfers of *personal data*, thus all other information that does not qualify as personal data is outside the scope of the right. This scope is problematic due to the contextual and variable nature of personal data, which leaves the right to data portability hanging on unstable ground.[8] Going further, Article 20(1) GDPR, in a joint interpretation with Recital 68, leads to the analysis that the scope of the right is limited to circumstances when the data subject has *provided* personal data to a controller. The lack of definition for the term "*provided*" evokes a series of legal discussions leading to different interpretations, with the narrowest one supporting only *volunteered data*[9] – which might include only personal data that the subject has *explicitly* provided, such as data collected through a registration form, or all data collected upon consent, such as location data and cookies –. Under a broader interpretation, the term "*provided"* would also include *observed data*[10] or data that was *derived or inferred* from observed or volunteered data, called *interred data.* The European Data Protection Board (EDPB) – former *Article 29 Working Party* – has defended a middle-ground interpretation of its interpretative guidelines on the right to data portability, stating that the right only includes *observed data,* excluding *inferred data*.[11] [12] De Hert et al., point out that Recital 68 clearly states that *"the right to data portability should apply where the data subject provided the personal data based on his or her consent or the processing is necessary for the performance of a contract"*, clarifying that not only data explicitly provided should be ported, but also data provided based on the data subject's consent or performance of

[3] The GDPR defines Personal data as "any information relating to an identified or identifiable natural person". Recital 26 GDPR mentions that in order to determine whether a person is identifiable, an account must be taken of all the reasonable means likely to be used, either by the data controller or by a third party, to identify, directly or indirectly, the person.

[4] Article 29 Working Party (2016) 'Guidelines on the right to data portability', WP 242, 13 December 2016.

[5] Council (2016) Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council 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 (General Data Protection Regulation), Brussels, 3 May 2016, OJ C 159/1, p. 89.

[6] Article 20 states the following *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has promised to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".*

[7] Paul De Hert et al., 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services', Computer Law & Security Review 34, no. 2 (1 April 2018): 193–203, https://doi.org/10.1016/j.clsr.2017.10.003

[8] Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union. https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en

[9] Volunteered data is the type of data which is the data that subjects are aware that they revealed to the controller, such as account data submitted through online forms

[10] Such as clicks and locations. See Jan Kraemer, 'Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations', SSRN Scholarly Paper (Rochester, NY, 25 November 2020), https://papers.ssrn.com/abstract=3742771.

[11] D. Gill and J. Metzger, 'Data Access Through Data Portability', European Data Protection Law Review 8, no. 2 (2022): 221–37, https://doi.org/10.21552/edpl/2022/2/9.

[12] There is still uncertainty if "metadata" is included within the right to data portability. Paul De Hert et al., 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services', Computer Law & Security Review 34, no. 2 (1 April 2018): 193–203, https://doi.org/10.1016/j.clsr.2017.10.003

a contract, therefore including cookies and location data.[13] Nevertheless, the uncertain approach offered by the GDPR due to its legal vagueness hinders the potential of the right to data portability to strongly influence the market through consumer action and increase competition. For this reason, there is a proposal to update the GDPR with broader and more detailed wording.[14]

Further, according to Article 20(1)(a) of the GDPR, the data subject will be able to exercise this right to data portability when the processing of personal data is based on *consent* or *a contract*, excluding other legal grounds for processing that are listed in Article 6 of GDPR such as compliance with a legal obligation, protection of vital interests, necessary to carry out a task in the public interest and a legitimate interest pursued by the controller or by a third party –.[15] The right to data portability in itself is composed by three different rights: (1) the first one is the right to receive data concerning the data subject which he/she provided, (2) the second is the right to transmit the data to another controller, and lastly, (3) the right to have personal data transmitted from one controller to the other, when technically feasible.[16] Data portability rights are exercisable via an email contact, which may seem bureaucratic since it is necessary to wait for a reply and wait for the transfer to take place if accepted. This method also excludes real-time continuous data portability of personal data, although Art. 20(1) GDPR states that the right should be free from "hindrance", the article does not mention any technical solution for the fulfilment of such data portability requests.[17] Although the EDPB has suggested a "one-click solution" achievable through the use of APIs,[18] the GDPR remains unclear about this aspect. As a form to broaden the impact in the market, the GDPR does not limit to which controller the data will be transmitted, applying the right from small and medium enterprises (SMEs) to companies that hold major economic power such as big techs. [19]

Data subjects can request the portability of data at any point in time, free of charge, yet there are three exceptions: (1) The right won't be exercised if the requested data was deleted or anonymized; (2) if the request interferes with a task carried out in the public interest, and (3) if the porting of data affects the *rights and freedoms of others*. Although the GDPR does not specify what would be considered the *rights and freedoms of others* and whether this interpretation is limited to natural persons, possible conflicts have emerged – such as economic and proprietary rights of the data controller, and the right to data protection of third persons –, the wording does not grant full prevalence of other rights on data portability, instead only a "non-prevalence" rule which will need to be determined on a case-by-case approach which will take into consideration future contexts.[20]

According to Article 6 (1)(a) GDPR, the right to data portability only includes data related *to the data subject which makes the request*, raising questions pertaining to the right to data protection of other data subjects on the hypothesis of having an entanglement of personal data of multiple individuals – e.g. In cases where multiple data subjects being portrayed in the same picture, would the portability of the relevant dataset contained in this wider dataset of personal data require the consent of third parties involved, or would only the relevant dataset exclusively

[13] De Hert et al.

[14] Geminn, Christian L. "Betroffenenrechte verbessern: Überarbeitungsbedarf der Datenschutz-Grundverordnung." Datenschutz und Datensicherheit-DuD 44, no. 5 (2020): 307-311.

[15] European Commission. (2017a). Guidelines of Article 29 Data Protection Working Party on the right to data portability (WP 242 rev.01). https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611233

[16] De Hert et al.

[17] D. Gill and J. Metzger.

[18] Article 29 Working Party (2016) 'Guidelines on the right to data portability', WP 242, 13 December 2016.

[19] The term "gatekeeper" here is applied as defined by the Digital Markets Act.

[20] De Hert et al.

concerning the data subject be extracted for exercising the individual right to data portability.[21] [22] In contrast, the EDPB takes the position that in such a situation the rights of a third party are not violated if the data is kept in the sole control of the requesting user and is managed for personal or household needs, thus according to this understanding, the controller should not deny the request if data subjects are requesting the download of data.[23] There is, therefore, major controversy when it comes to the intersection between the right to data portability and the right to data protection of other individuals still to be discussed and established.[24]

When it comes to technical standards of the right to portability, Article 20 of the GDPR is limited through its mention that data subjects have a right to obtain data in a *structured, commonly used and machine-readable format*.[25] According to the EDPB,[26] these terms must be considered to be minimal technical requirements, although Recital 68 explicitly mentions that no obligations are imposed on controllers for adopting specific data processing systems, while standardization is encouraged. [27] In practice, this lack of guidance can be considered a double-edged sword, while some sectors already have standard data formats established through industry practice, others do not and lack any guidance on that aspect.

Lastly, the GDPR does not allow the data controller to charge the data subjects for claiming their right to data portability, unless the data subject submits requests that are unfounded or excessive, however even in this case, according to Art. 12(5) of the GDPR, the imposed fee must be proportional, reasonable and based solely on administrative costs. Hence, considering the abovementioned points, it is possible to observe that the right to data portability seems to be the first step towards the direction of giving data subjects more control over their data, although there are major obstacles to implementing this right, especially in the field of competition law, it was based on this observation, the Digital Markets Act was proposed.

b) Introduction Of The Right To Data Portability Into The Commercial Ecosystems: The Digital Markets Act

The Digital Markets Act (DMA), has entered into force on 1 November 2022 and applies from 2 May 2023, introducing an *ad hoc* regulatory regime of the digital markets which complements the EU's and Member States' competition rules.[28] Having as a legal basis Article 114 of the Treaty on the Functioning of the European Union (TFEU), the Digital Markets Act faces the big tech concentration of data wealth[29] – a practice that either falls outside the existing EU competition rules or cannot be effectively addressed by them –, through the enforcement

---

[21] Janal, Ruth. "Data portability under the GDPR: A blueprint for access rights?." In Data Access, Consumer Interests and Public Welfare, pp. 319-342. Nomos Verlagsgesellschaft mbH & Co. KG, 2021.
[22] De Hert et al.
[23] Article 29 Working Party (2016) 'Guidelines on the right to data portability', WP 242, 13 December 2016.
[24] Such as the possible restriction of the right to data erasure. "Another risk might be that, in order to guarantee a full exercise of the right to data portability to all users, data subjects whose data are inseparable from other subjects' data could be prevented from having their data erased. In all these cases, Article 20(3) states a prevalence of right to erasure on the right to data portability". at Paul De Hert et al., 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services', Computer Law & Security Review 34, no. 2 (1 April 2018): 193–203, https://doi.org/10.1016/j.clsr.2017.10.003
[25] Art. 20(1) GDPR
[26] Article 29 Working Party (2016) 'Guidelines on the right to data portability', WP 242, 13 December 2016.
[27] Engels, Barbara. "Data portability among online platforms." *Internet policy review* 5, no. 2 (2016).
[28] EDPS Opinion on the European Commission's proposal for a Digital Markets Act. https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-markets-act_en
[29] Muhammed Demircan, 'The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions', SSRN Scholarly Paper (Rochester, NY, 8 December 2022), https://doi.org/10.2139/ssrn.4297229.

of an ex-ante regulatory instrument which shifts the *status quo* of the digital platforms and markets regulation.[30] While the GDPR is focused on the data subject's fundamental right to the protection of personal data, the DMA is centered around data as an economic asset, which initially might seem contradictory, but is the reflection of Article 16 of the TFEU.[31] [32]
The Digital Markets Act is an asymmetric regulation with a broad scope which encompasses different participants and stakeholders in the same industry[33] namely- *online intermediation services, online search engines, social networking, video-sharing platform services, number-independent interpersonal electronic communication services, operating systems, cloud services, and advertising services.*[34] All these firms share the same characteristics: extreme economies of scale, very strong network effects, and the ability to connect many business users with many end users through the wide applications and the multi-sidedness of these services.[35]

Once these stakeholders and participants are classified as a *gatekeeper* according to the requirements of Article 3 of the DMA, eighteen different obligations set across Articles 5 and 6 of the DMA are triggered, which aim to tackle issues of competition through the creation of data access rights.[36] Amongst these obligations, Article 6(9) DMA introduces a new data portability right which stipulates that gatekeepers shall provide end users and authorized third parties with *"effective portability of data provided by the end-user of generated through the activity of the end user"*.

At a first glance, the right to data portability introduced by the DMA seems to refer to the one introduced by the GDPR, although the DMA-induced right is limited to the activities of gatekeepers and the GDPR is restricted to the portability of provided personal data of data subjects. Therefore, the DMA does not introduce a new right to data portability, instead, it makes an addition to the right to data portability originally introduced by the GDPR, widening its ambit from the previously envisaged personal data to now cover *all data provided* by the end-user generated through his/her activity at a gatekeeper platform, including all legal bases listed in Article 6(1) GDPR. This indicates that the DMA covers both *personal* and *non-personal data inferred* and *derived* data, an assumption that finds echo in Recital 59 which states that end users and third parties should be granted access to the data provided or that was *generated through their activity*.[37] The portability of inferred data is considered to be essential for competition in the digital market, as it was recognized by the Federal Cartel Office of the

---

[30] Manuel Woersdoerfer, 'The Digital Markets Act and E.U. Competition Policy: A Critical Ordoliberal Evaluation', Philosophy of Management, 1 September 2022, https://doi.org/10.1007/s40926-022-00213-4.
[31] Article 16 TFEU "1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".
[32] Philipp Baschenhof, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?', SSRN Scholarly Paper (Rochester, NY, 11 August 2021), https://doi.org/10.2139/ssrn.3970101.
[33] Baschenhof.
[34] Article 2(2) DMA
[35] Digital Markets Act Explanatory Memorandum https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
[36] Baschenhof.
[37] Damien Geradin, Konstantina Bania, and Theano Karanikioti, 'The Interplay between the Digital Markets Act and the General Data Protection Regulation', SSRN Scholarly Paper (Rochester, NY, 29 August 2022), https://doi.org/10.2139/ssrn.4203907.

Düsseldorf Higher Regional Court Decision B6-22/16,[38] since competitors would not be able to replicate derived data otherwise.[39]

When it comes to technical details of the right to data portability, the DMA takes a more detailed approach as compared to the GDPR, since Recital 59 states that users have the right to *"(...) continuous and real-time access to such data"* provided in a format that *"can be immediately and effectively accessed and used by the end-user or the relevant third party authorized by the end user to which the data is ported"*. Recital 59 goes further, mentioning that gatekeepers also must ensure *high-quality technical measures* – such as application programming interfaces (APIs) – that permit the free porting of data continuously and in real-time. Therefore, the DMA has a *"plug-and-play"* right to data portability in mind, which is less bureaucratic and more effective in promoting market entry and competition,[40] in contrast with the bureaucratic and operationalization metrics heavy procedure offered by the GDPR. However, the DMA, much like the GDPR, does not provide any guidance on what data format or mechanisms must be used to port data, it is limited to say that to implement continuous and real-time data access, high-quality technical measures must be implemented by gatekeepers such as the previously mentioned APIs. This choice according to authors Gal and Rubinfeld, does not solve data portability problems, therefore the issues related to the lack of standardization in the GDPR remain in the DMA.[41]

According to Article 26(1) of the DMA, the European Commission shall take the necessary actions to monitor the effective implementation and compliance with the obligations laid down in Articles 5 and 6, including the right to data portability. In case of non-compliance, Article 29 (1) DMA states that the Commission shall implement a "non-compliance decision", requesting the gatekeeper to cease and desist from the ongoing non-compliance with the enforcement of the right to data portability.

At this point, it is necessary to highlight that while many provisions of the DMA openly refer to the GDPR, others remain unclear regarding its coherence. Thus, to make sense of this overlap, alongside the general principle *lex specialis derogate legi generali*, it is possible to refer to the European Court of Justice ruling in the *Joined Cases C-54/17* and *C-55/17* that state when the contents of EU law provisions overlap, the one that conducts a more detailed or applies to a specific sector will be applicable.[42] However, as Geradin et.al. point out, in practice uncertainties remain and data subjects/users would still need to make clear under what Regulation they are exercising the right to data portability.[43] When it comes to other possible tensions between the DMA with other national and EU rules, only time will tell, and possible case-by-case analysis will follow. Therefore, it is possible to observe that the Digital Markets Act brings the right to data portability a step forward in comparison to the GDPR.

---

[38] Bundeskartellamt [Federal Cartel Office] Feb. 6, 2019, B6-22/16 http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf%3F__blob%3DpublicationFile%26v%3D5

[39] Baschenhof.

[40] Jan Kraemer, 'Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations', SSRN Scholarly Paper (Rochester, NY, 25 November 2020), https://papers.ssrn.com/abstract=3742771.

[41] Michal S. Gal & Daniel L. Rubinfeld, Data Standardization, 94 N.Y.U. L. REV. 94, 737–770 (2019).

[42] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, [2021] OJ C 526/1 refers to Joined Cases C-54/17 and C-55/17, paragraphs 60-61.

[43] Geradin et.al.

c) The Necessary Evolution Of The Right To Data Portability Through A Collection-Centric Approach: The Data Act Proposal

The Data Act was the last proposed Act of the European Data Strategy, becoming public on February 2022, and is still being discussed at the time of the finalization of this paper.[44] According to Recital 4 of the Data Act Proposal, the main objective of the proposal is to remove the barriers to accessing data, laying down a harmonized framework which specifies who is entitled to access the data generated by products and related services. The scope of the Act includes *"manufacturers of products and suppliers of related services placed on the market in the Union, data holders and recipients, public sector bodies and Union institutions, agencies or bodies, providers of data processing services, operators within data spaces and vendors of applications using smart contracts"*, excluding providers of IoT products or related services that qualify as micro or small enterprises.

The Proposal covers any type of connected object which contains sensors that permits it to generate or collect data and communicate through the internet, including virtual assistants, excluding products that are designed to *display, play, record or transmit content such as personal computers, servers, tablets, and smartphones*; "smart watches" may be covered by the Regulation if they have the ability to communicate data via a publicly available electronic communication service.[45] Contrary to the GDPR and DMA, the Data Act avoids the dichotomy between personal and non-personal data,[46] including a broad spectrum of data through terminology which encompasses *all data generated* – thus, including personal and non-personal data – by the use of a product or related service, including data *intentionally* and *not intentionally* recorded by the user, diagnostics data, "standby mode" data and the data recorded when the product is switched off. Recital 14 mentions explicitly that data in raw form and prepared data – including metadata – is included, however, data that results from software processes are excluded from the Proposal due to intellectual property rights.

The Data Act Proposal does not adopt the term "right to data portability", different from the GDPR and the DMA, instead, the proposal adopts the term "data access", which also encompasses the right to data portability. Chapter II of the Data Act Proposal is fully dedicated to the rights of users[47] to use data of connected products and related services, separating the right to data portability between Articles 4 and 5, which must be interpreted alongside Recital 31, which is entirely focused on the connection between the Data Act with the GDPR, stating that the data generated by the use of a product or service should only be made available to a third party at the request of the user, *complementing* the right to data portability under Article 20 of the GDPR, including the right to receive personal data and port data to other controllers.

According to Recital 21, ideally, products may be designed to allow direct data access by users through on-device data storage, but Article 4 states where data cannot be directly accessed by the user the data holder shall make data available to the user through electronic means, *without undue delay, free of charge, easily, securely, in a structured, commonly used and in a machine-readable format, continuously* and in real-time. Subsequently, Article 5 regulates the right of the user to share data with third parties, by the request of the user or by a party acting on behalf of a user *without undue delay, free of charge, easily, securely, in a structured,*

[44] The version used by this paper is the Second Presidency compromise text of the Data Act, issued on October, 222.

[45] European Commission (2022a) 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), 23 February 2022, COM(2022) 68 final.

[46] Graef, Inge. et al. (2019) 'Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation', European Law Review 44, 605-21

[47] Article 2 (5) 'user' means a natural or legal person, including a data subject, that owns, rents or leases a product or receives a related services;

commonly used and in a machine-readable format, continuously and in real-time where applicable. Taking advantage of the division of the right to portability into two different Articles, the Proposal mandates that the right to portability exercised by the user must be free of charge, however, when the data is made available in business-to-business relations, Article 9 of the Data Act Proposal states that a reasonable compensation – which can include costs and investment required for making data available[48] – can be agreed.

However, Recitals 8 and 21 along with Article 3 are considered to be a delicate point of the Data Act Proposal due to the language which has been adopted. According to Kerber, it is possible to infer that the data holder will not necessarily be required to *provide a copy* of the data to a third party. Instead, the text of the Proposal makes it possible to interpret that this data can be accessed through the server of the manufacturer or cloud service provider, through *"in-situ"* access to data. Yet, the enactment of "*in-situ*" data access would dramatically change the landscape of the right to data portability in the Proposal, reducing it to a mere "*right to data access*", and keeping data in the control of the data holders, who can unilaterally decide whether data is available only through "*in-situ*" or through data portability.[49] In our opinion, the in-situ access argument becomes more fragile with the existence of Recital 31, and its explicit reference to the complementarity of the Data Act with the right provided under Article 20 GDPR. Thus, in our opinion, although a clearer choice of language would be advisable, the holistic interpretation of the proposal leads us to conclude that the in-situ access, if existent, does not hinder the right to data portability.

To implement these technical demands imposed by the Data Act, the Proposal does not ignore the fact that currently, not all data generated by products are easily accessible by users, thus Article 3 introduces the concept of *data access by design,* specifying that all IoT devices and related services have to be *designed*, *manufactured* and *provided* in a manner that facilitates the real-time, continuous accessibility of the data by the user directly, in an easy and secure manner. This concept is also essential for data protection purposes. Recital 20 states that manufacturers must make reasonable efforts in the design of the products so *all persons* have access to the data they generate, therefore the design should allow the separation of data that belongs to different persons that use the same device. This must be interpreted in conjunction with Article 4 which regulates that the *user*[50] has the right to access and use data generated by the use of a product or related service when the user *is not* the data subject whose personal data is requested, Article 4(5) dictates that the data shall only be made available where there is a valid legal basis under Article 6(1) of the GDPR (consent), and *where relevant* under conditions of Article 9 GDPR (conditions for the processing of special categories of personal data), and Article 5(3) of the e-Privacy Directive (consent to the storage of and access to cookies on users' devices) are fulfilled. To allow data access to the user, Recital 27 of the Data Act Proposal mentions that the data holder may require appropriate user identification.

The correlation between the Data Act and the GDPR is not only restricted to data protection of other data subjects besides the user but in Article 6 the Data Act Proposal mentions that a third party that receives the ported data must process personal data only for the purposes and under the conditions agreed with the user, deleting the data when they no longer are necessary for the agreed purpose, without hindering the effective application of the data access rights as per Recital 23 of the Data Act Proposal, thus incorporating the underlying principles of consent and lawful processing as well as retention of personal data enshrined in the GDPR to the legal fabric of the Data Act Proposal.

---

[48] Recital 42

[49] Kerber, Wolfgang. "Governance of IoT Data: Why the EU Data Act will not fulfill its objectives." *Available at SSRN 4080436* (2022).

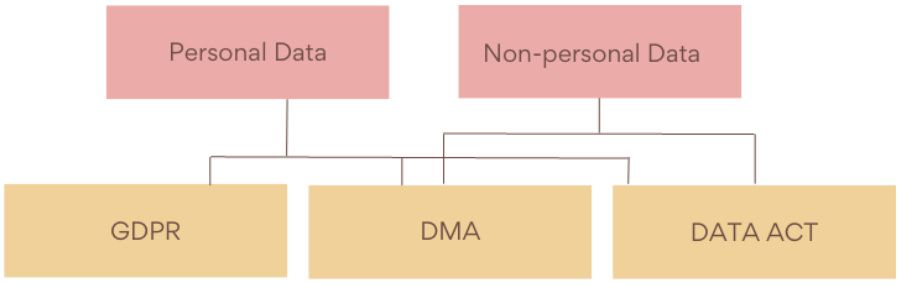
[50] Article 2 (5) of the Data Act Proposal: "'user' means a natural or legal person, including a data subject, that owns, rents or leases a product or receives a related services";

Finally, the original Data Act Proposal, proposed in February 2022, aims to achieve a data market balance by excluding gatekeepers from being able to receive data through the right to data portability under Article 5, this position makes sense due to the existing power imbalances on the data market. Nevertheless, it is essential to highlight that the Proposal is still under legislative proceedings and this position might be modified.

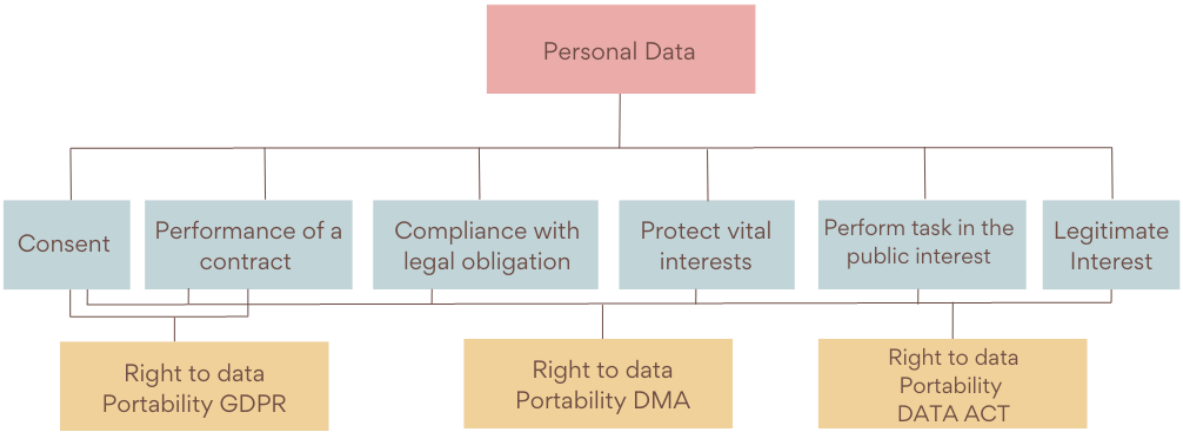
III. A Holistic Analysis Of The Right To Data Portability

The previous section focused on the outline of the main aspects of the right to data portability in the three regulations separately, exploring its rationale, scope, objectives, and limitations through a text-based analysis. This section aims to make an analysis of the correlations between the right to data portability in the three Regulations, taking into consideration the inferences made in the previous section.

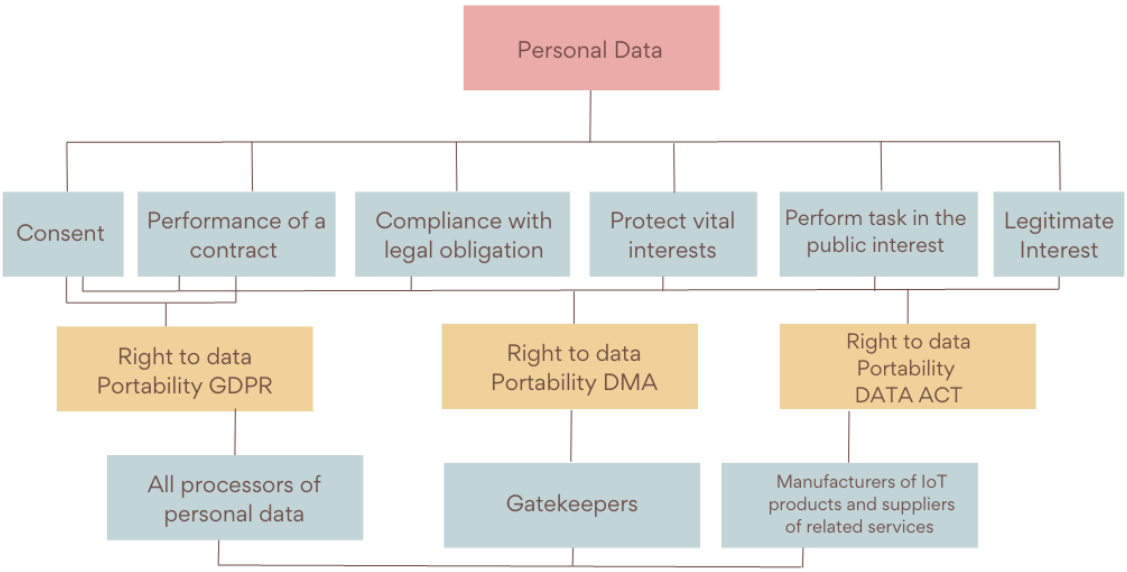
As regards the scope of data covered, there is an undeniable overlap and synchronism between the three Regulations, since the GDPR regulates the processing of personal data, and the Digital Markets Act and the Data Act include the processing of personal data and non-personal data by gatekeepers and IoT products manufacturers and services, respectively.



Focusing on the right to data portability of personal data, the synchronized overlaps between the Regulations are modified. The GDPR has the smallest scope of the three regulations since it is restricted to personal data that has been *provided* to a controller under the basis of *consent* or *contract*, whereas the DMA and the Data Act govern the processing of personal data *independently* of the lawful basis for processing.



When it comes to the processor under the scope of the regulations, the GDPR has the broadest scope of the three, having a broad scope that covers all categories of personal data processors, while the DMA scope is restricted to stakeholders which qualify as gatekeepers under the DMA and lastly, the scope of the application of the Data Act is restricted to IoT manufacturers and suppliers of related services, with the exception of SMEs.



Thus, even though there are clear observed overlaps between the GDPR, DMA and Data Act, doubts remain on how effectively they will work in the practical implementation of the right to data portability. It might be necessary to identify under which Regulation a data subject or user is requesting the right to data portability, especially if the basis of the request is personal data which has been processed based on consent or contract since this right of data portability could be enacted under the GDPR, DMA and Data Act. Yet, this will only be in fact visible when the three regulations are enforced at the same time in a particular instance.

IV- Concluding Remarks

The right to data portability is a right introduced by the GDPR that was deemed to be revolutionary due to its novelty and potential to give data subjects control over their data and potentially change the market landscape. Since its enactment, the right still finds a series of technical and legal interpretation-based obstacles that block its full implementation. Nevertheless, the option to give data subjects and users more control over their data has not been forgotten and is a critical endeavour envisaged under the European Data Strategy. In light of this, the right to data portability was also included in two Regulations (apart from the GDPR), namely the Data Markets Act and the currently pending Data Act Proposal. Along the various sections of this study, it is possible to observe that the right to data portability as envisaged under the three Regulations can be considered as different layers of the same right (emanating first from the GDPR) and is focused on giving individuals more control over their data, both-personal and non-personal, with the ultimate objective of breaking data monopolies and boosting the data market.

Since these three Regulations have different scopes and varying concepts, doubts still remain on how individuals will be able to effectively use the right to data portability in a way that is beneficial to them and the market, as easily and with as much ease as possible. Therefore, it is essential that the interpretation of the multi-layered right to data portability does not cause confusion and ends up hindering the right of individuals instead of giving them more opportunities, and although the "without prejudice" clause is present in the three regulations, often the intersection between different regulations cause misunderstandings. These misunderstandings will surface and will probably be solved on a case-by-case basis when the three regulations are enacted at the same time. The endeavours to create a three-tiered harmonious legal regulation governing a data subject's right to data portability through the symbiotic interpretation and applications of the GDPR, the DMA and the Data Act Proposal are underway and there are great expectations of not only legislative and regulatory re-alignment but also the appropriate industry adoption and operationalization of the right to data portability which has been duly streamlined and incentivized by the government and regulatory bodies and exercised by the data subjects.