EJLT European Journal of Law and Technology

The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act

Bárbara da Rosa Lazarotto[*]

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. Most recently, the Digital Markets Act and the Data Act have also introduced tertiary legal provisions building on the right to data portability, therefore adding previously unforeseen nuance. However, due to many factors, the right to data portability has found little or no practical application. 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 GDPR, the Digital Markets Act and the Data Act. 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.

Keywords: data portability, GDPR, Digital Markets Act, Data Act.

[*] Bárbara Lazarotto, PhD researcher at Vrije Universiteit Brussel. The author has received funding from the European Union's Horizon 2020 research and innovation programme under the GA no 956562.

1. Introduction

The digital economy has been the core of the European Data Strategy, due to the potential of data to benefit businesses, researchers and public administration. The subsequent transformation of the EU's economy impacts data-driven companies in particular, due to their special position in the digital information market and their often predatory and anti-competitive practices.[1] 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, hinder accessibility, and impede data subjects' control over their data through Regulations such as the General Data Protection Regulation (GDPR).

The sharing of data is considered to be a potential solution for ending such monopolies, as it was possible to observe in some EU sector-specific data access regimes, such as the Digital Content Directive, Electricity Directive and Payment Services Directive.[2] Yet, when it comes to personal data collected by platforms such as social media, several barriers still prevent an optimal sharing and transfer of data, such as a lack of incentives for data holders, legal uncertainties about the rights and obligations concerning data owing to broad legislative provisions, and an absence of universal standards for semantic and technical interoperability. In answer to this situation, the right to data portability *as a data protection derivative right* was introduced by the GDPR, 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 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 (DMA) and the Data Act 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.

In this context, the aim of this article is to explore the current landscape of the right to data portability as the derivative of the GDPR's right to data portability, with an examination of possible complementarities and conflicts between the GDPR, DMA and Data Act. It takes into consideration the underlying objectives of these three Regulations, with the purpose not only 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.

---

[1] Kraemer J, 'Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations' (2020) https://papers.ssrn.com/abstract=3742771 accessed 12 December 2022.

[2] Graef I, Husovec M, Van Den Boom J, 'Spill-overs in data governance: Uncovering the uneasy relationship between the GDPR's right to data portability and EU sector-specific data access regimes' (2020) 9 *Journal of European Consumer and Market Law* 1.

This article is structured as follows: following this introductory section, Section II will outline the main aspects of the right to data portability in the GDPR, DMA and Data Act, exploring their rationale, scope, objectives and limitations through a text-based analysis of three Regulations. Addressing the multiple interpretations of the texts, Section III will focus on a holistic analysis of the right to data portability, considering how the constructions of this right in these three Regulations may intersect with how they differ, and how these similarities and differences may impact its application by individuals, and consequently on the market. Finally, the Section IV concludes with a summary of the analysis and closing remarks.

2. 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: (1) the GDPR, which is already approved and entered into force in 2018; (2) the DMA, which entered into force on 1 November 2022 and applies from 2 May 2023; and (3) the Data Act, which entered into force on 11 January 2024 and becomes applicable in September 2025.

2.1 The Legal Debut of the Right to Data Portability: the General Data Protection Regulation

The GDPR was a paradigm shift regulation that entered into force on 25 May 2018, aiming to strengthen the general conditions for data processing, providing more precise definitions, and reinforcing accountability and liability of controllers, while enhancing processing responsibility.[3] Amongst these changes, the GDPR has introduced a series of new rights to empower data subjects, with the objective of giving them more control over their personal data while encouraging its flow within the EU.[4] [5]

The GDPR introduced the *right* to data portability in Article 18(1) of its initial proposal, intending to allow individuals to change online services more easily. As the proposal evolved within the legislative process, the right narrowed considerably, including only personal data that the individual had provided to the controller under the scope of the right.[6] As the GDPR proposal progressed, the right to data portability was

[3] Kuner C, Bygrave LA, Docksey C, 'Background and evolution of the EU general data protection regulation (GDPR)' in *The EU General Data Protection Regulation (GDPR)* (Oxford University Press, 2020).
[4] Article 29 Working Party, 'Guidelines on the Right to Data Portability' (2016).
[5] 'Statement of the Council's Reasons: 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)' (27 July 2016).
[6] Kuner et al (n 3).

consolidated in Article 20.[7] Today this right has taken a different shape than was initially intended, transforming into a mechanism used to strengthen individuals' ability to exercise self-determination over their data while facilitating competition among data controllers through the sharing of data.[8]

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 on unstable ground.[9] 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[10] – 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 or data that was derived or inferred from observed or volunteered data, i.e. interred data.[11] The European Data Protection Board (EDPB) – formerly the 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.[12] [13] 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 should data explicitly provided be ported, but also data provided based on the data subject's consent or performance of a contract, therefore including cookies and location data.[14] Nevertheless, the uncertain approach offered by the GDPR due to its legal vagueness hinders the potential of the right to

[7] Article 20 GDPR states: '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'. [2016] OJ L 119/1.

[8] De Hert P et al, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 *Computer Law & Security Review* 193.

[9] 'EDPS Comments on a Framework for the Free-flow of Non-personal Data in the EU' (European Data Protection Supervisor).

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

[11] Such as clicks and locations. See Kraemer J, 'Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations' (2020).

[12] Gill D and Metzger J, 'Data Access Through Data Portability' (2022) 8 *European Data Protection Law Review* 221.

[13] It is still unclear if 'metadata' is included within the right to data portability. See De Hert et al (n 8).

[14] Ibid.

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.[15]

Further, according to Article 20(1)(a) 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 GDPR, namely compliance with a legal obligation and protection of vital interests, necessary to carry out a task in the public interest and legitimate interest pursued by the controller or by a third party.[16] The right to data portability in itself is composed of three different rights: (1) the right to receive data concerning the data subject which he/she provided; (2) the right to transmit the data to another controller; and (3) the right to have personal data transmitted from one controller to the other, when technically feasible.[17] Data portability rights are exercisable via an email contact, which may seem bureaucratic since it is necessary to wait for a reply and for the transfer to take place if accepted. This method also excludes real-time continuous data portability of personal data, although Article 20(1) GDPR states that the right should be free from 'hindrance', it does not provide any technical solution for the fulfilment of such data portability requests.[18] Although the EDPB has suggested a 'one-click solution' achievable through the use of APIs,[19] the GDPR remains unclear about this aspect. As a means of broadening 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.[20]

Data subjects can request the portability of data at any point in time, free of charge, with three exceptions: (1) if the requested data is deleted or anonymised; (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 the 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, there is only a 'non-prevalence' rule, which will need to

[15] Geminn CL, 'Betroffenenrechte verbessern' (2020) 44 *Datenschutz und Datensicherheit – DuD* 307.
[16] European Commission, 'Guidelines of Article 29 Data Protection Working Party on the right to data portability' (WP 242 rev.01, 2017).
[17] De Hert et al (n 8).
[18] Gill and Metzger (n 12).
[19] Article 29 Working Party (n 4).
[20] The term 'gatekeeper' is applied as defined by the DMA. See Regulation (EC) 2022/1925 on contestable and fair markets in the digital sector [2022] OJ L149.

be determined on a case-by-case approach that takes into consideration future contexts.[21]

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 the personal data of multiple individuals becoming entangled. For example, in cases where multiple data subjects are 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 concerning the data subject be extracted for exercising the individual right to data portability?[22,23] 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 within the sole control of the requesting user and is managed for personal or household needs. According to this understanding, the controller should not deny the request if data subjects are requesting the download of data.[24] There is, therefore, the issue of the intersection between the right to data portability and the right to data protection of other individuals is controversial and requires further discussion.[25]

When it comes to technical standards of the right to portability, Article 20 GDPR is limited in its statement that data subjects have a right to obtain data in a *structured, commonly used and machine-readable format.*[26] According to the EDPB, these terms must be considered minimal technical requirements, although Recital 68 explicitly states that no obligations are imposed on controllers for adopting specific data processing systems, while standardisation is encouraged.[27] [28] In practice, this lack of guidance can be considered a double-edged sword; while standard data formats are already established through industry practice in some sectors, in others this has not happened and there is a lack of guidance.

Lastly, the GDPR does not allow the data controller to charge data subjects for claiming their right to data portability, unless the data subject submits requests that

---

[21] De Hert et al (n 8).

[22] Janal R, 'Data portability under the GDPR: A blueprint for access rights?' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos, 2021) 319–342.

[23] De Hert et al (n 8).

[24] Article 29 Working Party (n 4).

[25] 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 the right to erasure on the right to data portability.' See De Hert et al (n 8).

[26] Article 20(1) GDPR.

[27] Article 29 Working Party (n 4).

[28] Barbara Engels, 'Data Portability among Online Platforms' (2016) 5 *Internet Policy Review* https://policyreview.info/articles/analysis/data-portability-among-online-platforms accessed 12 January 2022.

are unfounded or excessive. However, even in such cases, under Article 12(5) GDPR, the imposed fee must be proportional, reasonable and based solely on administrative costs. Hence, considering these points, the right to data portability seems to be the first step towards 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 because of these obstacles that the DMA was proposed.

2.2 Introduction of the Right to Data Portability into Commercial Ecosystems: Digital Markets Act

The DMA 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 and Member States competition rules. With a legal basis Article 114 of the Treaty on the Functioning of the European Union (TFEU), the DMA addresses the challenges and systemic problems posed by the digital platform economy, especially the big tech concentration of data wealth – a practice that either falls outside the existing EU competition rules or cannot be effectively addressed by them – through the enforcement of an *ex ante* regulatory instrument which shifts the status quo of the digital platforms and markets regulation.[29,30,31] While the GDPR is focused on the data subject's fundamental right to the protection of personal data, the DMA is centred around data as an economic asset, which initially might seem contradictory, but is a reflection of Article 16 TFEU.[32]

The DMA is an asymmetric statute with a broad scope, which encompasses different participants and stakeholders in the same industry, 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*.[33,34] All these firms share the same characteristics: extreme economies of scale, very strong network effects, and the

[29] Bongartz P, Langenstein S and Podszun R, 'The digital markets act: moving from competition law to regulation for large gatekeepers' (2021) 10 *Journal of European Consumer and Market Law* 2.

[30] Dermican M, 'The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions' https://link.springer.com/chapter/10.1007/978-3-031-31971-6_12 accessed 27 January 2023.

[31] Woersdoerfer M, 'The Digital Markets Act and E.U. Competition Policy: A Critical Ordoliberal Evaluation' https://link.springer.com/article/10.1007/s40926-022-00213-4 accessed 27 January 2023.

[32] Baschenhof P, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?' (11 August 2021) https://papers.ssrn.com/abstract=3970101 accessed 12 February 2023.

[33] Baschenhof (n 32).

[34] Article 2(2) DMA.

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 'gatekeepers' according to the requirements of Article 3 DMA, eighteen different obligations set across Articles 5 and 6 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 authorised third parties with 'effective portability of data provided by the end-user of generated through the activity of the end user'.

At first glance, the right to data portability introduced by the DMA seems to refer to that 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 coverage from personal data to all data provided by the end-user generated through his/her activity on a gatekeeper platform, including all legal bases listed in Article 6(1) GDPR. This indicates that the DMA covers both personal and non-personal, inferred and derived data, an assumption echoed in Recital 59, which states that end users and third parties should be granted access to the data provided or which was generated through their activity.[37] The portability of inferred data is considered to be essential for competition in the digital market, as was recognised by the Federal Cartel Office of the Düsseldorf Higher Regional Court Decision B6-22/16, since competitors would not otherwise be able to replicate derived data.[38]

When it comes to the technical details of the right to data portability, the DMA takes a more detailed approach than the GDPR. 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, stating 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, in contrast with the bureaucratic and

[35] Explanatory Memorandum for the Proposed Regulation (EC) 2022/1925 on contestable and fair markets in the digital sector [2022] OJ L149
[36] Baschenhof (n 32).
[37] Geradin D, Bania K and Karanikioti T, 'The Interplay between the Digital Markets Act and the General Data Protection Regulation' (29 August 2022) https://papers.ssrn.com/abstract=4203907 accessed 12 February 2023.
[38] Bundeskartellamt [2019] B6-22/16, Feb 6.

operationalisation metrics-heavy procedure offered by the GDPR.[39] 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 only states 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 Gal and Rubinfeld, does not solve data portability problems; therefore the issues related to the lack of standardisation in the GDPR remain in the DMA.[40]

According to Article 26(1) DMA, the European Commission shall take the necessary action to monitor the effective implementation and compliance with the obligations laid down in Articles 5 and 6, including the right to data portability. In the 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, the coherence of some aspects is still doubted. Thus, to make sense of this overlap, alongside the general principle *lex specialis derogate legi generali*, we refer to the European Court of Justice ruling in the Joined Cases C-54/17 and C-55/17, which states that when the contents of EU law provisions overlap, the one that conducts a more detailed regulation or applies to a specific sector will be applicable.[41] 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.[42] When it comes to other possible tensions between the DMA and 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 DMA is ahead of the GDPR in bringing the right to data portability a step forward.

2.3 The Necessary Evolution of the Right to Data Portability through a Collection-Centric Approach: Data Act

The Data Act was the last proposed Act of the European Data Strategy, becoming public in February 2022, and adopted in November 2023. Its main objective is to establish a horizontal right of data access for private and business users of products by introducing mandatory business-to-business data-sharing contracts provisions.[43]

---

[39] KrämerJ, 'Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations' (2021) *Journal of Competition Law & Economics* https://academic.oup.com/jcle/article-abstract/17/2/263/6000371 accessed 27 February 2023.

[40] Gal MS and Rubinfeld DL, 'Data Standardization' (2019) 94 *New York University Law Review* 737.

[41] 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.

[42] Geradin et al (n 37).

[43] Metzger A and Schweitzer H, 'Shaping Markets: A Critical Evaluation of the Draft Data Act' (2022) *Zeitschrift für Europäisches Privatrecht*.

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 Act covers any type of connected object which contains sensors that permit it to generate or collect data and communicate through the internet, including virtual assistants, but 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. Contrary to the GDPR, the Data Act avoids the dichotomy between personal and non-personal data, including a broad spectrum of data through terminology which encompasses *all data generated* –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.[44] Recital 14 states that data in raw form and prepared data – including metadata – is included; however, data that results from software processes is excluded from the Act due to intellectual property rights.

Unlike the GDPR and the DMA, the Data Act does not adopt the term 'right to data portability'; instead, it introduces a horizontal cross-sectoral data access right to consumers and businesses that encompasses 'data generated by the use of the product or related services' (Chapter II). However, it emphasises the complementarity of this with the right to data portability in Articles 4 and 5 GDPR, interpreted alongside Recital 31, including the right to receive personal data and to 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. However, Article 4 states that 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, 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 Act mandates that the right to portability exercised by the user

[44] Graef I, Gellert R and Husovec M, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189 accessed 20 February 2023.

must be free of charge; however, when the data is made available in business-to-business relations, Article 9 Data Act states that a reasonable compensation – which may include the costs and investment required for making data available – can be agreed.[45]

However, Recitals 8 and 21 along with Article 3 are considered to be a delicate point of the Data Act due to the dubious 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, a possible interpretation of the Act is 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 Act, reducing it to a mere 'right to data access', and keeping data within the control of the data holders, who can unilaterally decide whether data is available only through in-situ access or through data portability. In our opinion, the in-situ access argument becomes more fragile in light 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 Act leads us to conclude that any in-situ access does not hinder the right to data portability.

To implement these technical demands imposed by the Data Act, it does not ignore the fact that, currently, not all data generated by products are easily accessible by users. 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 states that the *user* 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) GDPR (consent), and, where relevant, under conditions of Article 9 GDPR (conditions for the processing 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.[46] To allow data access to the user, Recital 27 Data Act states that the data holder may require appropriate user identification.

[45] Recital 42 Data Act.

[46] Article 2(5) DA: '" user" means a natural or legal person, including a data subject, that owns, rents or leases a product or receives related services'.

The correlation between the Data Act and the GDPR is not only restricted to data protection of other data subjects besides the user, but Article 6 Data Act states 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 are no longer are required for the agreed purpose, without hindering the effective application of the data access rights as per Recital 23 Data Act. This incorporates 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.

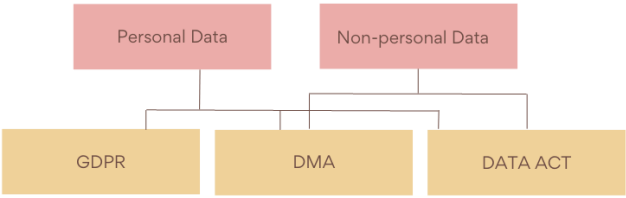
Finally, the original Data Act, proposed in February 2022, aimed to achieve a data market balance by excluding gatekeepers from receiving data through the right to data portability under Article 5. This position makes sense due to the existing power imbalances in the data market.

3. 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, exploring its rationale, scope, objectives and limitations through a text-based analysis. This section aims to analyse 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: the GDPR regulates the processing of personal data, and the DMA and the Data Act include the processing of personal data and non-personal data by gatekeepers and IoT product manufacturers and services, respectively (Figures 1 and 3). We can thus conclude that the GDPR has inaugurated the idea of a right to data portability, a right that was further developed in multiple other layers by the DMA and the Data Act.

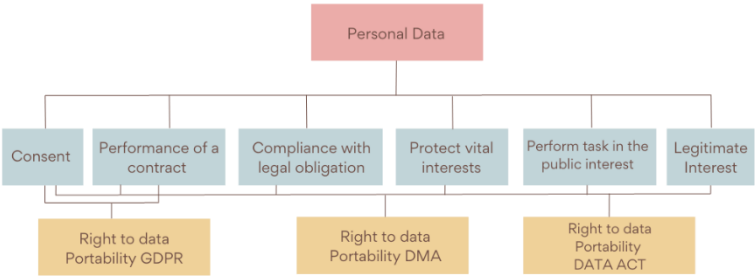
Figure 1: GDPR, DMA and Data Act process personal and non-personal data



Focusing on the right to data portability of personal data, the synchronised 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, being cross-sectoral regulations that encompass different technologies, especially the Data Act, that has a broad scope of IoT technologies (Figure 2).

Figure 2: The lawful basis for processing data and the different rights to data portability

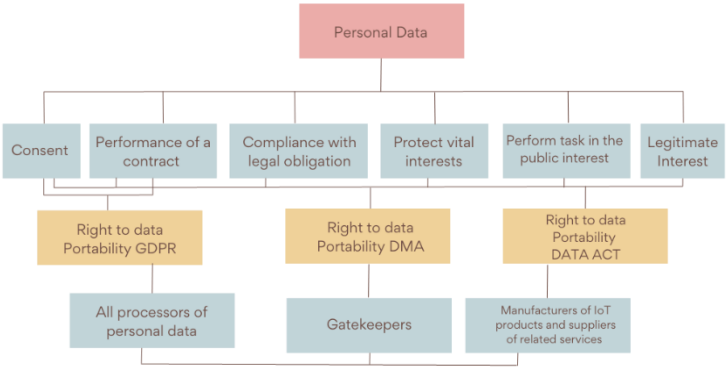


With the DMA, the Data Act has key connections and disconnections. First, the Data Act takes the concept of 'gatekeepers' from the DMA to deny them access to data portability requests (Article 5(2) Data Act), intending to expand the aftermarket services. At the same time, the Data Act goes beyond the DMA (and the GDPR) by creating a 'non-compete clause' for product users to incentivise the sharing of data (Article 6(e) Data Act).[47]

Under the three Regulations, the GDPR covers all categories of personal data processor, and so has the broadest scope of the three. The DMA's scope is restricted to stakeholders who qualify as gatekeepers under the Act, and the Data Act's scope is restricted to IoT manufacturers and suppliers of related services, with the exception of SMEs (Figure 3).

[47] Metzger and Schweitzer (n 43).

Figure 3: Stakeholders affecte by the different rights to data portability in the GDPR, DMA and Data Act



Thus, even though there are clear 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 become visible when the three Regulations are enforced at the same time in a particular instance.

4. Concluding Remarks

The right to data portability was introduced by the GDPR and was deemed 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, as this study has shown, it is possible to observe that the DMA and the Data Act can build new layers to this right with different, interconnected nuances.

By constructing a multi-layered right to data portability, individuals potentially have more control over their data – both personal and non-personal – in the context of a multi-sectoral setting, breaking data monopolies and boosting the data market.

Nevertheless, since the three Regulations have different scopes and varying concepts, doubts remain on how individuals will be able to effectively *exercise* the right to data portability in a way that is beneficial to them and the market, 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 hinder the rights of individuals instead of giving them more opportunities. Although the 'without prejudice' clause is present in the three Regulations, the intersection between different legislation often causes misunderstandings. These misunderstandings will undoubtedly surface and will probably be solved on a case-by-case basis when the three Regulations are enacted at the same time.

Endeavours to create a harmonious, three-tiered 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 are underway. There are great expectations of not only legislative and regulatory realignment, but also the appropriate industry adoption and operationalisation of the right to data portability, which has been duly streamlined and incentivised by the government and regulatory bodies, and exercised by the data subjects.