SITRA

MEMORANDUM

6 SEPTEMBER 2023

Sanna Toropainen

THE RIGHT TO DATA PORTABILITY IN THE FAIR DATA ECONOMY

Extending the right of individuals to benefit from managing their data

Sitra memorandum

**The right to data portability in the fair data economy –
Extending the right of individuals to benefit from managing their data**

Author: Sanna Toropainen

Sitra working group: Kristo Lehtonen, Meeri Toivanen, Reijo Aarnio, Johanna Kippo
Layout: PunaMusta Oy

ISBN 978-952-347-348-5 (PDF)
ISSN 2737-1034 (verkkojulkaisu)
www.sitra.fi

Sitra Memorandums are insights produced to support our future-oriented work.

Sitra memorandum
The right to data portability in the fair data economy
6 September 2023

Contents

Foreword

Digitally stored information, data, is the most valuable resource of our time. For us as individuals, our personal data tells a detailed story of who we are as consumers, voters or members of society. For business, data is crucial to optimising processes and developing innovative solutions to the big challenges facing us, from climate change and biodiversity loss to health crises and disinformation. We are witnessing a historic technological and economic transformation with advancements in digitalisation and an explosion of data transforming societies. Data has great potential for good, but we have a problem on our hands. The current data-driven economy is unfair because it magnifies the power of a few digital giants at the expense of individuals and society.

In the data economy, fairness means protecting the rights individuals and taking into account the needs of all stakeholders. We believe that in order to make the modern data economy fairer, we need new technological, economic and legislative innovations that specifically support the rights of individuals as the traditionally weakest party in the data economy. Currently, we 'pay' for the digital services that we use with our data and have little or no visibility into how the data we generate is used and by whom. For the data economy to work, we as individuals need to be able to control our data and our experience in the digital reality. Our ability to, for example, access our data and port it to a competing use is a fundamental pillar of a fair, human-centred data economy.

Privacy and consumer protection alone are not sufficient to meet this challenge. We also need an economic right for consumers in the fair data economy. In this study, we set out to investigate whether the principle of data portability could be part of the answer.

The European Union has introduced ambitious legislation for the data economy, starting with the General Data Protection Regulation (GDPR) in 2016. The GDPR introduced the right to port one's personal data, thereby helping to strengthen the position of individuals in the data economy vis-à-vis companies.

With the EU Data Strategy 2020, the European Commission has committed to taking further steps to enforce the principle of data portability in support of individuals in the data economy. Taken as a whole, the new data legislation and instruments that have emerged since the Data Strategy amount to a legislative tsunami. By harnessing the power of its internal market, the European Union is leading the way globally with its new regulation ('the Brussels effect'). One of the most ambitious proposals of the EU Data Strategy is the Data Act, which applies the principle of data portability to data generated by connected devices (Internet of Things, IoT), with a broader legal basis than the GDPR alone.

Ensuring that the principle of data portability can be enforced as easily and effectively as possible could be a way to support our digital sovereignty and make the data economy fairer for us all. This issue requires attention as the problem will become more difficult with new technologies such as virtual realities and the increasingly invasive tools associated with them, such as headsets. New ways of balancing the market power of digital giants with that of individuals and smaller companies are therefore needed more than ever.

We would like to thank Sanna Toropainen, the author, whose expertise as a legal expert in this field, as well as her background as a CEO and co-founder of a data intermediary, made her the perfect candidate to write this report. We would also like to thank the many people from the European Commission, member states, public authorities, NGOs and companies who took part in the roundtable we organised together with the European Policy Center (EPC) in Brussels in May 2023 as part of our Data Strategy 2.0 initiative, which resulted in recommendations for the next steps in European data policy. The progress of this report was significantly improved due to this interaction.

21 June 2023

Kristo Lehtonen
Director of the Fair Data Economy, Sitra

Reijo Aarnio
Senior Advisor, Sitra
Former Data Protection Ombudsman of Finland

Summary

The right of individuals to control their data must be strengthened as a basic right in the digital age, as proposed by Sitra in its recommendations for rectifying the imbalance of digital power (Sitra 2022a). The starting point is that individuals should be able to know what data is collected about them and how it is processed and shared, and to have a sovereign say in the process, including the right to data portability. The right to data portability is a way of redressing the current power imbalance between individuals and the technology providers that aggregate and monetise the data collected about individual users.

This paper argues that the right to data portability is a key element in the fair data economy because individuals should be active participants working alongside companies and institutions with a sovereign say on their data rather than just subjects in need of protection.

As the right to data portability is not an absolute right, but has to be balanced with other rights and freedoms, this paper first analyses the legal framework in the European Union governing the right to data portability. It concludes that the current framework risks taking a piecemeal approach to the right to data portability, both in substance and in enforcement, which could have a detrimental effect on the ability of individuals to fully exercising it.

Starting with the origin of the right in Article 20 of the General Data Protection Regulation (GDPR), the paper provides an overview of the legislative proposals that extend the scope of data portability from personal data to data generated by the use of connected devices and related services (the proposed Data Act) and to health data (the European Health Data Space), and looks at how the right is considered in the Digital Markets Act (DMA). The analysis shows how the proposed legislation broadens the scope of data portability to non-personal data and beyond data 'provided by' individuals, but at the same time remains limited due to sectoral application and limitations on the scope of Article 20 of the GDPR.

In addition to the legal framework, the paper identifies four current practical limitations to data portability: inadequate implementation by the companies, privacy and data security risks, lack of interoperability, and the unclear role of intermediaries.

Virtual realities and web 3.0 technologies are examined as a use case for data portability in light of the legal framework and the implementation challenges identified, because they represent an area for future technological developments with increased user involvement. While the decentralised decision-making of web 3.0 allows for more granular control over data and empowerment in the data economy, the virtual environment may pose new privacy risks due to the increased collection of sensitive data.

Lastly, the paper explores four ways in which the right to data portability could be strengthened to further the development of a fairer data economy in Europe through regulation. First, widening the scope of Article 20 of the GDPR beyond personal data 'provided by' the data subject to include inferred data could enable individuals to use the right more broadly. Thus, allowing individuals to port their data regardless of the legal base, would enable individuals to invoke the right against public authorities. Second, expanding the scope of Article 20 of the GDPR beyond personal data to include non-personal data (mixed data sets) would reflect the dynamic nature of data, and could ensure that the right to data portability works effectively in practice. Third, the right to data portability could be 'added' to the EU Charter of Fundamental Rights, alongside the right to privacy and data protection, to include both the right to control one's own data and the right to the economic benefits from data. Finally, new legislation with a specific definition of the data that can be transferred, and with a sufficiently broad application could improve the self-determination of individuals with regard to their data.

Tiivistelmä

Yksilöiden oikeutta hallita omaa dataansa tulee vahvistaa digitaalisen ajan perusoikeutena, kuten Sitra on esittänyt suosituksissaan digitaalisen vallan epätasapainon korjaamiseksi (Sitra 2022a). Lähtökohtana on, että yksilön tulee voida tietää, mitä dataa hänestä kerätään ja miten sitä käsitellään ja jaetaan. Hänellä tulee myös olla todellinen mahdollisuus vaikuttaa datan keruun ja käsittelyn eri vaiheissa sekä mahdollisuus siirtää häntä koskevaa dataa järjestelmästä toiseen. Oikeus siirtää dataa järjestelmästä toiseen on yksi tapa pyrkiä korjaamaan nykyistä vallan epätasapainoa yksilöiden ja heistä kerättyä dataa yhdistelevien ja sillä ansaitsevien teknologiatoimittajien välillä.

Tässä muistiossa todetaan, että oikeus datan siirtämiseen on keskeinen osa reilua datataloutta, koska myös yksilöiden tulisi olla aktiivisia toimijoita datataloudessa yritysten ja instituutioiden rinnalla. Heillä tulisi olla päätäntävaltaa heistä kerättyyn ja heitä koskevaan dataan sen sijaan, että heitä pidetään vain suojaamista tarvitsevina osapuolina.

Oikeus datan siirtämiseen ei ole absoluuttinen oikeus, vaan se tulee tasapainottaa suhteessa muihin oikeuksiin ja vapauksiin. Muistiossa analysoidaan ensin Euroopan unionin lainsäädännöllistä viitekehystä, joka koskee datan siirtämistä. Johtopäätöksenä on, että nykyinen lainsäädäntökehys lähestyy datan siirtämisen oikeutta sirpaleisesti, olipa kyse sitten tuon oikeuden sisällöstä tai toimeenpanosta. Tämä voi vaikeuttaa yksilöiden mahdollisuuksia käyttää täysimääräisesti oikeuttaan oman datansa siirtämiseen.

Oikeus datan siirtämiseen on lähtöisin yleisen tietosuoja-asetuksen (GDPR) artiklasta 20. Muistio luo katsauksen sitä seuranneisiin lainsäädäntöehdotuksiin datan siirtämisen oikeuden laajentamisesta. Niissä se ulottuisi kattamaan henkilötietojen lisäksi myös verkkoon kytkettyjen laitteiden ja palveluiden käytössä syntynyttä dataa (komission ehdotus datasäädökseksi) ja terveysdataa (komission ehdotus eurooppalaisesta terveystietoalueesta). Muistio käy myös läpi, miten EU:n digimarkkinasäädös (DMA) käsittelee oikeutta datan siirtämiseen. Analyysi osoittaa, miten ehdotettu lainsäädäntö kokonaisuutena ulottaa oikeuden datan siirtämiseen koskemaan muutakin dataa kuin vain henkilötietoja ja ihmisten ”antamia” tietoja. Samanaikaisesti oikeutta datan siirtämiseen rajaavat toimialakohtaiset erot toimeenpanossa ja GDPR:n artikla 20:n asettamat rajoitukset.

Oikeudellisen tarkastelun lisäksi muistiossa nostetaan esiin neljä käytännön rajoitusta datan siirtämiselle. Näitä ovat puutteellinen toteutus yrityksissä, yksityisyydensuojaan ja tietoturvaan liittyvät riskit, puutteet yhteentoimivuudessa ja välittäjäpalveluiden roolien epäselvyys.

Virtuaalitodellisuudet ja web 3.0 -teknologiat tarjoavat mahdollisuuden tarkastella datan siirtämisen soveltamista oikeudellisen kehyksen ja tunnistettujen käytännön haasteiden kautta. Ne edustavat tulevan teknologisen kehityksen aluetta, jossa käyttäjien osallisuudella on entistäkin keskeisempi rooli. Web 3.0:n hajautettu päätöksenteko mahdollistaa datan hienojakoisemman hallinnan ja yksilön vahvemman päätösvallan toteutumisen datatalousdessa. Samalla virtuaaliympäristö ja siihen liittyvä kasvava arkaluontoisen datan keruu saattavat aiheuttaa uusia uhkia yksityisyydensuojalle.

Lopuksi muistiossa ehdotetaan neljää mahdollisuutta, joilla oikeutta datan siirtämiseen voidaan vahvistaa ja siten edistää reilumman datatalouden kehitystä sääntelyn avulla Euroopan unionissa. Ensinnäkin GDPR:n artiklaa 20 voisi laajentaa niin, että se koskisi yksilöiden ”antamien” henkilötietojen lisäksi myös ”yhdisteltyä” dataa. Tämän lisäksi artikla 20:n soveltamisalaa tulisi laajentaa niin, että yksilöt voisivat käyttää oikeutta henkilötietojen käsittelyperustasta riippumatta, jotta he voisivat käyttää datan siirto-oikeutta myös suhteessa julkisen sektorin toimijoihin. Toisena vaihtoehtona on GDPR:n artiklan 20 ulottaminen koskemaan myös muuta dataa kuin henkilötietoja (nk. yhdistetyt data-aineistot), jolloin se ottaisi huomioon datan monimuotoisen luonteen. Näin voitaisiin varmistaa, että oikeus datan siirtämiseen toimii tehokkaasti käytännössä. Kolmanneksi oikeus datan siirtämiseen voitaisiin liittää Euroopan unionin perusoikeuskirjaan yksityisyyden suojan ja tietosuojan lisäksi erillisenä oikeutena. Se voisi pitää sisällään oikeuden hallita omaa dataansa ja oikeuden siitä saataviin taloudellisiin hyötyihin. Neljäntenä vaihtoehtona on uusi lainsäädäntö, joka määrittäisi tarkasti, millaista dataa voidaan siirtää ja jonka soveltamisala olisi kuitenkin riittävän laaja. Tämä voisi parantaa ihmisten mahdollisuutta päättää heitä koskevan datan käytöstä.

Sammanfattning

Individens rätt att kontrollera sina egna data måste stärkas som en grundläggande rättighet i den digitala tidsåldern, vilket Sitra föreslagit i sina rekommendationer för korrigering av obalansen i den digitala makten (Sitra 2022a). Den bakomliggande idén är att individer ska ha möjlighet att veta vilken data om dem som samlas in, bearbetas och delas. De måste också ha en verklig möjlighet att påverka de olika stadierna av insamlingen och behandlingen av data samt möjligheten att överföra data om dem från ett system till ett annat. Rätten att överföra data från ett system till ett annat är ett sätt att ta itu med den nuvarande maktobalansen mellan individer och de teknikleverantörer som kombinerar och tjänar pengar på data som samlats in från dem.

Det här dokumentet hävdar att rätten till dataportabilitet är ett nyckelelement inom den rättvisa dataekonomin eftersom individer bör vara aktiva deltagare som arbetar tillsammans med företag och institutioner, med ett avgörande inflytande över sina data snarare än att bara vara subjekt i behov av skydd.

Eftersom rätten till dataportabilitet inte är en absolut rättighet utan måste balanseras mot andra rättigheter och friheter, börjar detta dokument med att analysera den rättsliga ramen i Europeiska unionen som styr denna rättighet. Slutsatsen är att det nuvarande ramverket riskerar att anta ett styckevis förhållningssätt till rätten till dataportabilitet både i sak och efterlevnad, vilket kan få skadliga effekter för individer som utnyttjar sin rätt till dataportabilitet fullt ut.

Med utgångspunkt i ursprunget till rättigheten i artikel 20 i den allmänna dataskyddsförordningen (GDPR), ger dokumentet en översikt över de lagförslag som utökar omfattningen av dataportabilitet från personuppgifter till data som genereras genom användning av anslutna enheter och relaterade enheter och tjänster (den föreslagna datalagen) och till hälsodata (Den europeiska hälsodatarymden) samt tittar på hur rätten beaktas i EU:s rättsakt om digitala marknaders dataportabilitet (DMA, Digital Markets Act).

Analysen pekar på hur de föreslagna lagstiftningsakterna utökar omfattningen av dataportabilitet till icke-personliga uppgifter och bortom uppgifter som "tillhandahålls av" individerna, men samtidigt förblir begränsade på grund av sektoriell tillämpning och begränsningar vad gäller tillämpningsområdet för artikel 20 i GDPR.

Utöver den rättsliga ramen observerar dokumentet fyra nuvarande begränsningar för dataportabilitet från praxis: otillräcklig implementering av företagen, risker för integritet och datasäkerhet, bristande kompabilitet och mellanhändernas oklara roll.

VR- och webb 3.0-tekniker undersöks som ett användningsfall för dataportabilitet mot det rättsliga ramverket och de identifierade implementeringsutmaningarna eftersom de representerar ett område för framtida tek-

nisk utveckling med intensifierad användarmedverkan. Där decentraliserat beslutsfattande inom webb 3.0 möjliggör mer detaljerad kontroll över data och självbestämmande i dataekonomin, kan den virtuella miljön utgöra nya typer av integritetsrisker på grund av en ökande datainsamling av känslig data.

Slutligen undersöker artikeln fyra möjligheter till att förbättra rätten till dataportabilitet för att genom reglering främja utvecklingen av en mer rättvis dataekonomi i Europa. För det första kunde artikel 20 i GDPR utvidgas på så sätt att den gällde utöver personuppgifter som individer ”gett” även ”kombinerad” data. Dessutom bör tillämpningsområdet för artikel 20 utvidgas så att individerna kan utöva sin rättighet oavsett på vilken grund deras personuppgifter behandlas, så att de kan utöva rätten till dataportabilitet även i förhållande till aktörer inom den offentliga sektorn. För det andra, en utvidgning av tillämpningsområdet för artikel 20 i GDPR utöver personuppgifter till att även omfatta icke-personliga uppgifter (blandade datauppsättningar) skulle återspegla uppgifternas dynamiska natur och skulle kunna säkerställa att rätten till dataportabilitet fungerar effektivt i praktiken. För det tredje, rätten till dataportabilitet skulle kunna “läggas till” i EU:s stadga om de grundläggande rättigheterna vid sidan av rätten till privatliv och dataskydd, omfattande både självbestämmande (kontrollerande) av sin data och rätten till de ekonomiska fördelarna hos denna data. Slutligen kan ny lagstiftning med en specifik definition av de uppgifter som kan porteras och med en tillräckligt bred tillämpning förbättra individers självbestämmande när det gäller deras uppgifter.

1. Introduction

The amount of data that each individual creates through everyday actions, choices and preferences in the digitalised environment is growing exponentially. This data can be a valuable resource to innovate both better services and solutions that could respond to, for example, climate, biodiversity, and natural resources crises. However, it is important to include individuals as active participants in the data economy and place their interest first (European Commission 2020a). In this context, the European Commission talks about the data economy, which it defines as a part of the economy in which business is based wholly or largely on the use and exploitation of data in different ways by ensuring that data is accessible and usable (European Commission 2017a).

In the European Union, the data-driven transition is based on European values and fairness. In this sense, fairness in the data economy means that the rights of individuals are protected, and that the needs of all stakeholders are taken into account in a balanced way. One aspect of this is the right to data portability.

The right to data portability, as described in Article 20 of the GDPR, allows European citizens to receive the personal data a company processes about them and transmit that data to another company. The right to data portability reinforces the right of access, Article 15 of the GDPR, which guarantees that individuals have information about the processing of their personal data. As such, the GDPR is the first horizontal legislation to introduce the right to transfer one's data from one system to another.

The right to data portability is a tool to redress the power imbalance between individuals and technology providers (De Hert et al. 2018). The research conducted by Sitra confirmed that individuals have little control over the use of their data, while a small number of US-based technology companies have concentrated economic power, which they accumulate by aggregating user data and monetising it through advertising infrastructure (Sitra 2022a).

Most of this data is collected with the consent of individuals, using so-called cookie technology, which tracks users across websites. The use of cookies has been criticised for a lack of transparency – individuals rarely understand that they are consenting to the transfer of their personal data to a third party and what the consequences are (European Commission 2017b). Consumer organisations are calling for the EU to revise the rules on cookies and to adopt the proposal for the ePrivacy Regulation rapidly, as the proposal was already introduced in 2017 (BEUC 2021). In its current form, however, the proposal for the ePrivacy Regulation does not address the issue of the distribution of wealth from the data collected through cookies and risks restoring the current status quo of the (unfair) data economy.

In contrast to the current ePrivacy Regulation proposal, data portability promises an opportunity for individuals to 'share the wealth created by big data' and gain sovereignty over their data (Article 29 Working Party 2014).

However, the adoption of the right to portability has been low, both in the business sector due to a lack of incentives and among individuals due to a lack of awareness. The reasons for the low adoption of data portability after the entry into force of the GDPR can be attributed to, among others, the limited scope of the right, challenges in the technical application of the right, and the lack of interoperability of different services, which hinders the usability of the right if individuals cannot take their personal data from one platform to another (European Commission 2020a).

In 2022, the European Commission presented two new legislative proposals that, once adopted, strengthen the right to data portability for individuals, the Data Act and the European Health Data Space Regulation (EHDS). The former regulates access to and sharing of data from connected devices (European Commission 2022a). The latter will ensure the portability of health data and its secondary use (European Commission 2022c).

The new proposals aim precisely to share the value created from data more equitably between businesses of different sizes and individuals who generate the data as data subjects. This should lead to a more competitive and better functioning market for data sharing in Europe, where the GDPR and its Article 20 are primarily tools to enforce the fundamental rights of individuals.

A risk is that the new proposals create a piecemeal approach to data portability, where the scope of the right is contextual and too complex for individuals to operationalise (Tombal and Graef 2023). This complexity around the right to data portability further increases with new technological trends such as the metaverse and Web 3.0, which on the one hand enable users to have greater control through distributed decision-making processes in digital environments, and on the other could lead to an exponential collection of sensitive and behavioural data from users.

This paper aims to facilitate the discussion on achieving an actionable and comprehensive right to data portability for individuals. It responds to the research questions: 'What are the main legal and technical limitations to the right to data portability?' and 'How should the legal framework for data portability be changed to achieve an actionable and comprehensive right to data portability?'. The research has been carried out through desk research on the current laws, proposed legislation and EU policy documents, and by reflecting on recent academic discussions on the subject.

The paper looks at the European legal framework for data portability in order to identify some of the critical legal issues that limit the usefulness of the right for individuals (Section 2) and examines the main technical limitations of the right to data portability (Section 3). The paper also analyses those limitations in the context of the metaverse and Web 3.0 (Section 4). Finally, the paper presents four hypothetical ways to improve the right to data portability to overcome the challenges that it identifies (Section 5).

The Data Act and the EHDS also regulate data sharing between businesses and between a business and a government. The discussion in this paper is limited to examining the right to data portability for individuals. The proposed ePrivacy Regulation also falls outside the scope of this paper, because it does not provide for portability rights.

2. The right to data portability in the European Union

The European Data Strategy (Commission 2020a) defines data portability as an important tool to empower individuals with regard to their data and enable them to 'decide at a granular level what is done with their data', making reference to 'personal data spaces' as a way to connect to the data ecosystem via data portability. Indeed, individuals can use data portability to switch services and transfer their data to a new service, request a second opinion based on the ported data, or use complementary services such as gaining new insights from their consumption data.

This chapter examines the legal framework in the European Union for data portability from the perspective of an individual. The assessment looks at the extent to which different legal instruments in the EU address the right to data portability and their combined effect. The scope is limited to the GDPR, the Data Act proposal, the European Health Data Space (EHDS) proposal and the Digital Markets Act (DMA).

2.1. Article 20 of the GDPR

The General Data Protection Regulation (GDPR) in a nutshell

What is the GDPR about? The GDPR harmonises the protection of the fundamental rights and freedoms of EU citizens with regard to the processing of their personal data. The protection of personal data is guaranteed by Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). The GDPR was adopted in 2016 in response to the global development of technology, which poses new challenges to the protection of personal data, for example due to the rapid increase of data collection by companies and digitalisation of the economy and social life (Recital 6 GDPR).

What is a data subject? According to Article 4(1) of the GDPR, a data subject is a natural person, whose personal data is processed by a data controller or processor. A data controller is a natural or legal person, public authority, agency or other body that "determines the purposes and means" of the processing (Article 4(7) of the GDPR), and a data processor is a natural or legal person (or other) that processes personal data on behalf of the controller (Article 4(8) GDPR).

What are the data subject's rights? The GDPR provides for eight rights of the data subject, empowering individuals in relation to their data and giving them concrete tools to control their personal data. In addition to the right to data portability, the rights include, for example, the right to obtain information on the processing of personal data, right of access, right to be forgotten and right to object to the processing of personal data.

What does the GDPR say about data portability? Article 20 GDPR guarantees that individuals have the right to receive personal data, and the right to transmit that data to a third party. The article obliges companies to provide personal data in a structured, commonly used, and machine-readable format (Article 20(1) GDPR). If a company does not respond to the data portability request, an individual can complain to a data protection authority (DPA) in their Member State (Article 77 GDPR). The DPA may impose administrative fines in case of non-compliance according to Article 83 of the GDPR.

The GDPR can be seen as the main source of the right to data portability in the EU. However, it is not without limitations. The review of the GDPR in 2020 revealed that although individuals are "increasingly aware of their rights", the right to data portability is not being fully used (European Commission 2020b).

Three of the issues hindering the effective use of the right are discussed here: the limited scope of Article 20, the limited legal basis of Article 20 and the balancing of the right with the rights and freedoms of others.

The limited scope of Article 20 of the GDPR

First, the GDPR applies to personal data, which is defined in Article 4(1) of the GDPR as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, with identifiers such as name, location data, or other factors such as physical or psychological. The Working Party 29 guidance further clarified that the notion of personal data should be interpreted broadly (Article 29 Working Party 2007).

The WP29 identifies four elements that are relevant in determining whether a piece of information is personal data. These elements are:

1. "any information" referring to any statement about an individual
2. "relating to" referring to when information is about an individual
3. "an identified or identifiable" referring to a person who can be identified directly or indirectly by means of identifiers
4. "natural person" refers to a living individual

Article 20 limits the scope of the portability to include only data "provided by" the data subject. Hence, the point of contention has been what data

is included in the definition "provided by". This means personal data that the individual provides 'knowingly and actively' and personal data they generate by themselves. According to the WP29, this also refers to the "observed data" that the company receives when the data subject uses its service or device. Such data could be search history, traffic data, location data, or data from a wearable device, such as heartbeat data recorded by a device (Article 29 Working Party 2007).

The definition "provided by" can be contrasted to "inferred" or "derived" data, where a data controller creates user profiles based on the information the individual provides to the company, either voluntarily or through the use of a product or service (Article 29 Working Party 2017). Thus, individuals do not have the right to port their user profiles or any behavioural analysis a company has conducted using proprietary algorithms. They can nevertheless request information about the profiling logic and recipients of the personal data under Article 15 GDPR. Graef et al. (2019) contend that the scope limitation "undoubtedly cause difficulties for the data subjects" to make use of the data portability, because it is unclear what data will be included in addition to the raw data.

The limited legal basis of Article 20 of the GDPR

Second, for individuals, the usability of the right to data portability is further limited because Article 20 of the GDPR only applies in situations where a controller has obtained consent from the data subject for the data processing or the processing is based on a contract with the user (Article 2(1) and (2) GDPR). Therefore, individuals cannot use the right to portability against public authorities that process personal data. It has been proposed that this is because the right to portability is considered an "economic right", and there was no consideration when the GDPR was adopted that individuals could benefit economically from porting data from public authorities (De Hert et al. 2018).

Relationship with other rights and freedoms

Third, the right to data portability is not an absolute right, so in responding to a data portability request, a company must assess whether responding would violate the rights and freedoms of others (Article 20(4) GDPR). For example, suppose an individual requests to port personal data from Facebook. In this case, the dataset cannot include posts made by other people, even if the person has commented on them, or if porting the data would infringe the confidentiality of the data or intellectual property rights relating to the data.

However, from a business perspective, the limitation is welcome as it limits the conflict with data holders' intellectual property rights, such as copyrights, trade secrets and *sui generis* database rights. Graef et al. (2019) note that it prevents competition from benefiting from the ready-made con-

sumer profiles or from reverse-engineering an algorithm from inferred data, should a user wish to transmit personal data to another service provider. Although the Article 29 Working Party reminds that business risk is not enough to refuse a data porting request, the company is obliged to find a way to share data so that it does not disclose trade secrets or confidential data (Article 29 Working Party 2017).

This brief analysis shows that the right to data portability under Article 20 of the GDPR has a limited scope. Solove (2023) notes that "on many sites where data portability would be most desired by users, there will be significant limitations on how much data be ported and how useful porting data will be". In this sense, the regulation of data portability reflects the challenges that regulators face with new, rapidly developing technologies – much will depend on regulators' understanding of the technologies involved and the possibilities for data portability.

2.2. Article 4 and 5 of the Data Act

The Data Act in a nutshell

What is the Data Act about? The European Commission published the proposal for the Data Act in 2022. The Act is one of the cornerstones of the European Data Strategy, facilitating data sharing and data innovation in Europe. In April 2023, the final version of the proposed Data Act was under negotiation by the European Council and the European Parliament (European Parliament 2023a). The text of the proposal is therefore subject to change.

What is connected device data? The Data Act harmonises the rules on "making data generated through the use of a product or related service available by data holder to data recipients and on the making data available" (Article 1(1) Data Act). Connected devices, also known as the Internet of Things (IoT), refers to all physical products that receive, generate, or collect data and can communicate and exchange the data (Recital 14 of the Data Act). The Act regulates access to and use of data in business-to-consumer, business-to-business and business-to-government relationships, but micro or small enterprises are excluded from the scope (Article 7(1) Data Act).

What does the Data Act say about data portability? Article 4 of the Data Act sets out the conditions under which individuals can request access to and use of data generated by connected devices and related services. Article 5 ensures that users can share data with a third party, either by themselves or by using data intermediary services as defined in the Data Governance Act (DGA). For example, an individual using a smart thermostat can request that the electricity provider share their electricity consumption profile with a comparison service (Thombal and Graef 2023).

Manufacturers are obliged to provide the data "without undue delay, easily, securely, in a comprehensive, structured, commonly used, and machine-readable format, free of charge, when feasible continuously and in real-time, including information required in Article 15 GDPR about the purpose of the processing and recipients of the personal data, and relevant metadata (that is necessary to interpret and use the data)" (Article 4(1) Data Act).

The Data Act proposal is a response to a market failure caused by the lack of access to IoT data by those who generate it (European Commission 2022a). For example, car manufacturers have control over vehicle data and an upper hand in aftermarket services and repairs because the data is processed through the manufacturer's proprietary system (Gill and Metzger 2020).

The proposal thus creates obligations for manufacturers of connected devices and providers of related services to make data available and, upon request by a user to transmit that data to a third party (Articles 4 and 5 of the Data Act). The Data Act also enables the development of aftermarket services, repair, and other complementary services when the data is shared with third parties as well as addressing lock-in situations where users are deterred from switching to a new platform due to the inconvenience of losing all existing connections, content, and data (European Commission 2022b).

The right to data portability in the Data Act versus the GDPR

The Data Act broadens the application of the portability to data generated through the use of connected devices. In the context of connected devices, individuals will have the ability to port personal and non-personal data regardless of the legal basis for the processing. In contrast to Article 20 of the GDPR, the Data Act concerns "any data" the user generates through the use of products or related services (Article 2(1) Data Act). Therefore, personal and non-personal data are included in the scope, as long as there is a valid legal basis for the processing of personal data. The broad definition of data also includes data from all digital assets, including apps, virtual machines and "manifestations of virtualization technologies", including metadata (Fernandez 2022).

Where Article 20 GDPR was limited to data "provided by the individual", the Data Act also includes data "generated as a by-product of the user's action, such as diagnostic data, and without any action by the user, such as when the product is in 'standby mode' and data recorded during periods when the products is switched off" (Recital 17 of the Data Act). However, according to the compromise text adopted by the European Parliament,

Article 4(1) will exclude data derived or inferred using complex algorithms (European Parliament 2023b).

Enforcement of the right to data portability through the Data Act versus the GDPR

Article 31(1) of the Data Act requires EU member states to appoint an authority responsible for the application and enforcement of the regulation. Each member state can decide on the composition of the authority, whether to create a new authority or whether to have multiple authorities. An individual will be able to complain to the authority about breaches of the Data Act (Article 31(3)(b)). If the issue concerns the processing of personal data, the competent authority will be the relevant data protection authority in each member state, in accordance with the GDPR (Article 31(2)(a) of the Data Act).

Krämer et al. (2023) describe the creation of new authorities to oversee the data regulations, such as the Data Act and the Data Governance Act, a "decentralised enforcement model" that carries the risk of confusion. How will the different authorities ensure effective co-operation, so that individual can have their complaints heard and dealt with promptly – especially in situations where it is unclear, whether it should be the authority responsible for enforcing the Data Act and/or the Data Protection Authority.

Hierarchy between the Data Act and the GDPR

According to Tombal and Graef (2023) an individual can rely on both Article 20 of the GDPR and the Data Act to port and transmit personal data generated through the use of connected devices. Their understanding is that "the Commission views the GDPR as containing a *de minimis* data portability right with a broad scope of application, on top of which more specific and narrower, but arguably more 'powerful', portability rights (such as the IoT data access right) can exist".

However, the European Consumer Organisation notes that the proposed Data Act does not explicitly mention which legislation prevails in case of conflicting provisions – contrary to Article 1(3) of the Data Governance Act (BEUC 2023). Article 1(3) of the Data Act nevertheless states that the Act complements Article 20 of the GDPR "where users are the data subjects of personal data". According to Ducuing (2022), this means that if Article 20 of the GDPR is the relevant provision to be relied upon for the porting of personal data, then the provisions of the GDPR will clash with the proposed Data Act due to the limited scope of the data portability right under the GDPR. She concludes that once the Data Act is adopted, individuals will be able to have access to more data (beyond that "provided by" the data subject) than with Article 20 GDPR. However, individuals will still be prevented from being able to port user-profiles, and the interplay between Article 4 and 5 of the Data Act and Article 20 of the GDPR remains unclear.

2.3. Article 3 of the EHDS

The European Commission published the proposal for a European Health Data Space (EHDS) in 2022 to facilitate the primary and secondary use of electronic health data in the European Union. The proposed regulation strengthens the right of individuals to data portability in the health sector by helping them to control their electronic health data.

In Recital 11 of the EHDS, the legislator acknowledges the shortcomings of Article 20 of the GDPR in the healthcare sector for two reasons. First, individuals are not entitled to port their diagnoses and tests, because these are considered to be inferred and derived data that is excluded from the scope of Article 20 of the GDPR. Second, personal data collected, processed and stored by public authorities, including public health care providers, are excluded from the scope of Article 20 of the GDPR.

Article 3(1) of the EHDS gives individuals the right to access their personal electronic health data immediately, free of charge, and in an easily readable, consolidated, and accessible form. Article 3(8) EHDS allows individuals to transmit electronic health data to another provider or, alternatively, to have access to their health records. Similar to the right of access, the transmission should be done immediately, free of charge and without hindrance. However, under Article 3(3) of the EHDS, EU member states may restrict the scope of the right in accordance with Article 23 of the GDPR if necessary for patient safety and ethics.

The EHDS covers both personal and non-personal electronic health data, irrespective of the legal basis for processing of personal data. Personal electronic health data is considered as health and genetic data as defined by the GDPR, as well as data "referring to determinants of health, or data processed in relation to the provision of healthcare services, processed in an electronic form" (Article 2(2)(a) of the EHDS). Recital 5 of the EHDS also specifies that that the scope includes "inferred and derived data, such as diagnostics, tests and medical examinations, as well as data, observed and recorded by automatic means".

Pop and Grant (2023) welcome the broadening of the scope of Article 20 of the GDPR by the EHDS proposal. However, they question whether the EHDS will encourage greater circulation of sensitive data if individuals can port the inferred diagnostics from one healthcare platform and transmit it to another platform, which can share with other third parties within the limits of lawful processing. This may conflict with the data minimisation principle introduced by the GDPR (EDPB-EDPS 2023).

2.4. Digital Markets Act

The EU aims to curb the significant power of the largest technology providers with the Digital Markets Act (DMA), adopted in 2022. The Act uses the term "gatekeeper" to refer to core platform services such as online search engines, social networking services, video sharing platforms and web browsers (Article 2 of the DMA).

The DMA empowers the European Commission to designate which providers fall within the definition of gatekeeper and must comply with the obligations set out in the DMA (Article 3 and 4 of the DMA). These obligations include prohibiting the combination of personal data from the core service with third-party services and prohibiting the cross-use of personal data between the core service and other services (Article 5 DMA). However, individuals may give their consent to the combination and cross-use of data (Article 3(1)(3) of the DMA).

In addition, under Article 6(9) of the DMA, gatekeepers are obliged to facilitate, free of charge, the effective data portability "of data that is provided by the end-user or generated through the activity of the end user in the context of the use" of the platform. The data should be made available in a format that "can be immediately and effectively assessed and used by the user or the relevant third party authorised by the end user to which the data is ported" (Recital 59 of the DMA). Thus, the gatekeeper must provide, free of charge, data portability tools that allow continuous and real-time access to data. The tools include application programme interfaces (Recital 59 of the DMA). The EU considers that these obligations will ensure that gatekeepers will not restrict switching or multi-homing of guarantees. If the gatekeepers do not comply with the obligations, they may be fined up to 10 % of their worldwide turnover (Article 30 of the DMA).

2.5. Comparison of rights

Table 1 gives an overview of the four instruments discussed in this paper, namely Article 20 GDPR, the Data Act proposal, the EHDS proposal and the Digital Markets Act.

Table 1. Comparison of the portability right

	ARTICLE 20 GDPR	DATA ACT PROPOSAL	EHDS PROPOSAL	DMA
Type of data	Personal data provided by the data subject	Personal and non-personal IoT data, that is derived and inferred	Personal and non-personal electronic health data, that is derived, inferred and observed	Data provided by the user or generated in the context of use
Legal base	Contract and consent	NA	NA	NA
Technical requirements	Structured, commonly used, and machine-readable format	Structured, commonly used, and machine-readable format	Electronic copy, in the European electronic health record exchange format	Continuous, real-time access by the user or authorised third party
Target of the request	Any controller regardless of the activity	Manufacturers of connected devices and providers of related services	An entity or a body in the health or care sector, or performing research in relation to these sectors (private or public)	Gatekeepers

3. Limitations to the right to data portability

The legal framework for the right to data portability is being expanded through the introduction of the proposed Data Act and the EHDS. Nevertheless, once adopted, proposals will create a piecemeal right to portability that will need to overcome the technical and non-technical limitations that have hindered the effective use of Article 20 of the GDPR.

This paper discusses four limitations: inadequate implementation of the right by companies, privacy and data security risks, lack of interoperability, and the role of intermediaries.

Limitation 1: Inadequate implementation by companies

The exercisability of the right to data portability has been questioned due to the non-implementation of the tools to port data. For example, Wong and Henderson (2019) have studied the responses of 230 data controllers to data portability requests. Their specific focus was on the right to receive data rather than the right to transmit it. The research findings showed that portability requests were cumbersome to complete, with around 75 per cent and of the 230 data controllers completing the request. Researchers also received the data in various formats that did not comply with the technical requirements set in Article 20, such as PNG screenshots and PDF scans that were not machine-readable as required.

A recent study published in 2022 also found that out of 160 privacy policies for IoT devices, only a small proportion explained the right, and when researchers tested popular devices, none enabled porting data to another device (Turner et al. 2021). The study focused on IoT products available in the UK, such as fitness trackers Garmin Vívosmart 4 and Fitbit Change 3, and home assistants Amazon Echo and Google Home.

Wong and Henderson (2019) read the fact that companies still need to implement data portability policies and processes, and that only a few relevant court cases have addressed aspects of data portability, as a sign of low consumer interest in data portability. It remains to be seen whether the Data Act and EHDS will revive interest and fulfil the high expectations placed on data portability as a means of promoting fair competition. If individuals do not make use of the right, there is no benefit for competition and the market for complementary services.

Limitation 2: Privacy and data security risks

While data portability can be a tool for empowerment and increase the ability of users to uphold their right to privacy and data protection, it can also create horizontal privacy imbalances. When the data is ported from one platform to another, it is taken out of context. If the ported data includes personal data, the question is, whether the legal, technical, and social constraints apply to the new platform. Data portability is not a legitimate reason for processing personal data, but at the same time, data portability does not prevent the misuse of data. (Hondagneu-Messner 2021.)

Privacy is also at risk if the data controller or the third party does not take adequate measures to protect the data in transit (as well as at rest). Privacy is even more at risk if a company grants the wrong person access to the data (Swire 2020). It is thus relevant to ask how individuals are identified when data is requested to be ported or transmitted to another party. The GDPR, for example, does not prescribe requirements for user authentication, but Recital 57 of the GDPR states that "identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller".

Limitation 3: Lack of interoperability

One of the reasons for the low use of Article 20 of the GDPR is the lack of value that individuals can create when porting their data. The value increases, however, if the individual can transmit this data to another service. Switching services also benefits competing companies by avoiding lock-in effects. However, there have been few incentives for companies to allow seamless transfer of customer data as it is more beneficial for the service to keep users on its platform and make it difficult to switch services, thus increasing user retention (OECD 2021).

In addition, the interoperability (syntactic and semantic) requirements increase costs for companies, especially as they need to ensure the right data format and security measures for transmitting the data. It is therefore essential to facilitate and incentivise interoperability, without which data portability loses its utility. So far, the GDPR has only encouraged companies to exchange files in interoperable formats, and there does not seem to be a requirement to develop a format that allows data to be transferred to another provider, as Recital 68 of the GDPR states that transfer is only required if 'technically feasible'. (De Hert et al. 2018.).

Limitation 4: Unclear role of intermediaries

Data intermediaries can remedy the lack of interoperability by enabling individuals to port their data to another provider by accessing and transferring it through intermediaries such as private services of Personal Information Management Systems (PIMS). PIMS can assist in the continuous transfer of data and facilitate translation into different formats, acting as "the single point of contact for users to control the data collection permission" (OECD 2021).

PIMS can also enable monetary compensation for data access by aggregating data and selling access rights on behalf of individuals. One example is a mobile app called DIMO, which monetises in-vehicle data. Another example is an Italian company called Hoda, which provides individuals with an application called Weople. The app allows individuals to link accounts such as Google's Gmail and others and port data into a 'digital vault'. Individuals can then earn virtual currency for authorising access to their vault.

Many of the PIMS, such as DIMO and Weople, are in the early stages of developing their operational and business models, and the regulatory framework is also under development. The recently adopted Data Governance Act (DGA) aims to instil trust in data intermediation by imposing constraints on the intermediaries' business models, requiring them to separate the data sharing from their core business in order to maintain neutrality (Article 11 DGA). On the one hand, the DGA is a first attempt to provide legal certainty to data intermediation; while on the other, it can be questioned whether the DGA imposes unnecessary constraints on the provider's freedom to provide business as guaranteed by Article 16 of the EU Charter of Fundamental Rights and whether it regulates an immature market (Ducuing 2022).

Questions also remain about the extent to which intermediaries help achieve data autonomy and self-determination in the fair data economy. Most PIMS claim to "give back control" to users over their data (like DIMO). Thus, intermediary services rely on consent as a legal basis for processing personal data. However, consent can be seen as *de facto* weakening "the protection of individuals because the data subject may not always have the best abilities or resources to decide on the processing of data" (Lindroos-Hovinheimo 2022) – especially in an environment that exploits the individuals' cognitive biases and nudges them to act in the desired way (Mäihänniemi 2022b).

There may also be also cases, for instance, where individuals are prompted to transmit personal data to services without understanding the consequences or being able to assess whether the company has taken sufficient measures to protect the personal data or whether the company will

share the data with another party. Also, if the individual withdraws consent and requests data to be deleted, will both the intermediary and the third party with whom the data was shared delete the data?

The use of consent has thus been criticised for placing the responsibility on the user, as the weaker party, instead of having a regulation that places the responsibility on the stronger party, the data controllers (Mäihänniemi 2022b). Cravo compellingly concludes 'that if individuals do not understand what they consent to, the economic benefit from the data portability can come with the loss of privacy' (Cravo 2022).

4. Use case: The data portability right in the metaverse

Having explored the legal framework for the right to data portability in the European Union, and the limitations that impede the full implementation of the right from four different perspectives, this section looks at the relationship between data portability and future technologies – namely, the metaverse and web 3.0.

What is a metaverse?

Sitra (2023) defines metaverse(s) as persistent virtual spaces that make use of decentralised decision-making, which can take form through such things as decentralised autonomous organisations (DAO) or by trading cryptocurrencies or non-fungible tokens (NFT). An example of decentralised virtual space is Decentraland, where users buy virtual land using NFTs developed on the Ethereum blockchain. Applications based on decentralised decision-making are also referred to as the next development phase of the internet, Web 3.0 (Sitra 2023).

Another example is the metaverse built by Mark Zuckerberg, who rebranded Facebook as Meta in 20211, to reflect the investment into building a social media metaverse (Facebook 2021a). Zuckerberg described the experience as "you'll move across these experiences on different devices – augmented reality glasses to stay present in the physical world, virtual reality to be fully immersed, and phones and computers to jump in from existing platforms" (Facebook 2021b). While in 2023, both Decentraland and Meta's Metaverse reported low user adoption (Paul 2023), the underlying technology and the idea of metaverses provide compelling use case for data portability.

How is data portability relevant in metaverses?

As discussed above, data portability has two distinct aims. On the one hand, it is a way for individuals to participate more in equal terms, as autonomous actors, in the data economy and benefit from the value potential of their data. But it is also a tool of fundamental rights, facilitating the right to data protection (under Article 20 of the GDPR).

Regarding the first aim, the question is whether individuals can benefit from the right to data portability in metaverses, and whether the right can help individuals to create value from their data. As an example of a fair data

economy pilot situated in the metaverse, Sitra, together with the Finnish National Gallery, curated the first ever metaverse exhibition on a Decentralised Autonomous Organisation (DAO) (Sitra 2023b). The stage for the experiment is a virtual replica of the Finnish Pavilion at the 1900 Paris World Fair, and it was created on the largest DAO in the world, Decentraland, where the art work on display could be minted into non-fungible tokens (NFTs) ready for exchange. If users ever wanted to move from Decentraland to a competing virtual world with, among other things, their NFTs, there might be interest in porting their data with them.

Under Article 20 of the GDPR, individuals will be able to port the personal data they generate in the virtual space. However, if virtual reality (VR) devices, such as VR headsets, are considered connected devices that collect, process and send data, they may fall under the scope of the proposed Data Act. As such, it will broaden the portability right to non-personal data generated by the device.

Currently, individuals have a limited ability to switch between metaverses because interoperability between the metaverses is almost non-existent, with each metaverse building its own protocols. As a result, individuals cannot benefit from their data or digital property (NFTs) ported to another metaverse (European Parliament 2022).

But could individuals benefit from porting the data and transferring it to an intermediary that creates complementary services when using metaverses? In the banking sector, individuals can, for example, benefit from services that analyse their banking data (Ferretti 2022). The VR headsets make it possible to track the users' location, body movements, facial expressions, and other biometric information, but the user may not be able to benefit from this data after switching service providers.

Meta has also launched its own VR headset, Meta Quest, which has five inward-facing cameras that allow avatars to display real-time expressions, smiles and winks. The new Apple Vision Pro mixed reality headset has similar capabilities. Could individuals port the data and transmit it to a third party? What value could data intermediaries help them to achieve by analysing the granular behavioural data? For example, could an intermediary help create consumer profiles that the individual could monetise using apps such as Weople? Also, central to the metaverse is the ability of the user to exert control over the data that they created. For example, modern VR headsets record data from human faces for long periods of time, so could the user provide their own data to support medical research? Should and could individuals port this data under the EHDS?

The value creation nevertheless is offset by the "unprecedented" privacy concerns that merge from the integration between the physical and virtual worlds (Nair et al. 2020). Nair et al. (2020) facilitated a small-scale study of metaverse user behaviour. They found out that users had difficulty understanding the breadth of data harvesting and how it could be used for targeted advertising, emotional exploitation, and political influencing. Nair et al. thus question the circumstances in which individuals give their consent to data

processing. Could there be a risk of users being 'lured' into porting their data to intermediaries that would then use it maliciously? Their findings also showed that even from anonymous profiles, it is possible to identify the user very quickly with only a few attributes (the longer the user stays on the platform, the easier it is to identify them).

The privacy risks accumulate rapidly in metaverses, considering the sensitive nature of the data that they can collect, including gender, sexual orientation, race, health data and disability, even as the decentralised technologies allow individuals to manage data flows and usage "based on individual free choice and self-determination" (Commission 2020a). As a solution, Anidjar et al. (2023) recommend that there should be "mandatory disclosure obligations with regulatory authorities on the protection they afford to users' privacy", but this in itself would not change the underlying logic of the data economy.

5. How can the right to data portability be improved?

The aim of this paper has been to examine how the new legislative proposals, the Data Act and EHDS, broaden the right to data portability and whether this broadening is sufficient for the right to reach its goals of user empowerment and enhanced competition from an individual's perspective. The analysis shows that the piecemeal approach to data portability creates gaps and overlapping rights to data. The following section considers four ways in which the data portability framework could be revised to encourage the development of a fairer data economy in Europe.

Option 1: Could the scope of Article 20 of the GDPR be broadened?

Article 20 of the GDPR is limited, among other things, to personal data "provided by" the data subject, and so far the article has had a minimal impact on building a fair data economy. For example, Gill and Metzger (2022) conclude that the scope of Article 20 limits the self-determination of individuals regarding their data since they cannot control data created through their actions. Thus, in their view, "if this right remains inefficient, data subjects will only have very limited control over their data as they are not able to gain a fair share of the value created from the data they have generated through their activities. Consequently, data sovereignty is not achieved".

The obvious improvement would be to broaden the scope of Article 20 of the GDPR to include inferred data and enable individuals to use the right regardless of the legal basis, so that individuals could also invoke the right against public authorities.

Option 2: Could Article 20 of the GDPR include personal and non-personal data?

The EU is moving away from the dichotomy between personal and non-personal data, as evidenced by the Data Act and the EHDS proposals. In practice, datasets are almost always mixed, containing data from both categories, and the definition of personal data is a moving target (see, for example, CJEU judgments *Breyer* and *Nowak).*

Graef (2019) argues that "due to its open-ended, fluid and dynamic nature, the notion of non-personal data is unlikely to become a useful defining criterion upon which firms can build their inputs for innovative products". She suggests that there should be a "holistic approach" without separat-

ing personal and non-personal data. One possibility could thus be to broaden the scope of Article 20 to include personal and non-personal data to ensure that the right is effective also in practice.

Option 3: Should there be a new right to data portability?

As we have seen, the right to data portability emphasises control and has a different economic objective than other data subject rights guaranteed in the GDPR. Some scholars even say that data portability is "a first step to an idea of data subjects" default *ownership* of their personal data (De Hert et al. 2018). Legal scholars have rejected the idea of regulating data as property because data is, among others, non-rivalrous and non-depletable (for example Van Erp 2021). Still, it is interesting to imagine whether the right to data portability could be 'added' to the EU Charter of Fundamental Rights alongside the right to privacy and data protection.

As a fundamental right, the right to portability would reflect the notion that individuals are entitled to the economic benefit of the data they produce. This view is supported by the findings of Sitra's study on tracking 'digital power', which highlights how individuals lack control over the data collection and how large technology companies, such as Meta and Google, are able to extract enormous economic value from profiling the users of their services (Sitra 2022a). The study recommends that the right to our 'own' data should be seen as a fundamental right to overcome the lack of control individuals face in the data economy. However, the right to data portability would encompass both the right to control one's data and the right to the economic benefits derived from it.

Further research is needed to understand the feasibility of such a proposal, but to achieve a fair data economy, individuals must be active participants and not just subjects in need of protection.

Option 4: A new legal instrument for data portability?

Another option could be to develop new legislation with a specific definition of the data that can be ported and a sufficiently broad scope ('any data', 'across all sectors', 'any product') to improve the empowerment of individuals with regard to their data. The instrument could be placed within consumer protection law, and it could take into account the different cognitive abilities of individuals when making decisions online, which that are compromised by the way the digital environment is designed to exploit individuals' cognitive biases. Under consumer protection, individuals are seen as the 'weaker party' and awarded more protection (Benöhr 2013).

In addition, although it was beyond the scope of this paper to examine the proposed ePrivacy Regulation, it is worth highlighting that there is a risk that individuals will continue to transfer their data to third parties through cookies without being aware of it and materialising the value they generate for companies. Therefore, the ePrivacy proposal should also be reviewed in terms of data portability.

6. Conclusions

The aim of this paper has been, first, to examine how the new legislative proposals, the Data Act and the EHDS, expand the right to data portability from the scope of Article 20 of the GDPR, and, second, what are the limitations for individuals to use the right effectively. The analysis of the expanded legal framework for the right to data portability shows that while the proposed Data Act and the EHDS will give individuals new rights to port their data in relation to data generated by connected devices and health data records, the application of these rights will remain sector specific. They complement Article 20 of the GDPR, which entitles individuals to port and transmit their personal data to third parties, but cannot remedy the limited scope of the provision itself.

It is questionable whether individuals will be able to achieve the economic objective of data portability with the limited, sector-specific scope. Technical limitations also hinder the usability of the right, and incentives for companies to develop interoperable services need to be increased. Data intermediaries, such as PIMS, can play a central role in helping individuals to create value from their data, but there are two risks.

The first risk is that the EU regulates an immature market where intermediaries are still discovering their business models and users. However, in the absence of regulation, there is a risk that consumers will not trust the data intermediaries and that the potential benefits of data intermediaries for consumer welfare will not be explored in the EU.

Intermediaries also play a role in technology trends such as the metaverse and Web 3.0, which are equally concerned with attracting users and developing the market. Individuals have a real chance to gain more control over their data with decentralised technology. However, this benefit needs to be weighed against the risk of losing autonomy through the increased collection of sensitive data in virtual realities (such as through VR headsets) and a digital environment designed to exploit user's cognitive biases.

The second risk is that by stressing the role of intermediaries the user's consent is further emphasised in legitimising data transfers. The question is whether this places more responsibility on individuals to understand the risks associated with data sharing without proper mechanisms to seek redress. The complex 'decentralised' structure of authorities in charge of the compliance of each data-related legislation (such as the Data Act, the Data Governance Act and the GDPR) also threatens effective redress for data misuse or lack of portability measures for individuals.

Accordingly, data portability is essentially a question of how to create a fair data economy where individuals are autonomous and self-sovereign over their data. Expanding the scope of the right to data portability with the Data

Act and the EHDS is a step in the right direction, but more is needed to rectify the limited application of Article 20 of the GDPR.

Therefore, this paper has explored hypothetical alternatives for a full right to data portability. Out of the four options, the most ambitious solution would be to add a new fundamental right, a right to data portability, alongside privacy and data protection. This would highlight the economic and other rights of individuals in relation to their data and their right to benefit from the data they generate in the digital environment, and would be a real step toward a fairer data economy.

References

EU legislation

Database Directive. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27 March 1996.

DGA. 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 (Data Governance Act), OJ L 152/1, 3 June 2022.

DMA. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265/1, 12 October 2022.

ePrivacy Directive. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002.

GDPR. 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 (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

CJEU case law

Peter Nowak v Data Protection Commissioner (C-434/16) [2016] ECLI:EU:C:2017:994

Patrick Breyer v Bundesrepublik Deutschland (C-582/14) [2014] ECLI:EU:C:2016:779

Secondary sources

Anidjar et al. 2023. The Matrix of Privacy: Data Infrastructure in the AI-powered metaverse. Harvard Law & Policy Review, Forthcoming. Last accessed on 10 May 2023.

Article 29 Working Party 2007. Opinion 4/2007 on the concept of personal data. WP 136, 20 June 2007. Last accessed on 30 June 2023.

Article 29 Working Party 2014. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. WP 217, 9 April 2014. Last accessed on 30 June 2023.

Article 29 Working Party 2017. Guidelines on the right to data portability. WP 242 rev.01, 5 April 2017. Last accessed on 30 June 2023.

The European Consumer Organisation (BEUC) 2021. Recommendations for the trilogue negotiations on the proposed e-Privacy Regulation. BEUC-X-2021-106. Last accessed on 16 May 2023.

The European Consumer Organisation (BEUC) 2022. Giving consumers control of their data - BEUC position paper on the Data Act proposal. BEUC-X-2022-103. Last accessed on 10 May 2023.

Benöhr 2023. EU Consumer Law and Human Rights. Oxford University Press, Oxford. Last accessed on 30 June 2023.

Colangelo 2022. European Proposal for a Data Act: A First Assessment. CERRE Assessment Paper, July 2022. Last accessed on 10 May 2023.

Cravo 2022. How to make data portability right more meaningful for data subjects? European Data Protection Law Review, 8(1), 52–60. Last accessed on 30 June 2023.

De Hert et al. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 193-203. Last accessed on 30 June 2023.

Ducuing et al. 2022. White Paper on the Data Act Proposal. CiTiP Working Paper 2022. Last accessed on 10 May 2023.

EDPB-EDPS 2022. Joint Opinion 2/2022 on the Proposal of the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). 4 May 2022. Last accessed on 10 May 2023.

European Commission 2017a. Building a European Data Economy. COM(2017) 9 final.

European Commission 2017b. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications. COM(2017) 10 final.

European Commission 2020a. A European strategy for data. COM(2020) 66.

European Commission 2020b. Communication from the Commission to the European Parliament and the Council data protection as a pillar of citizens' empowerment and the EU's Approach to the digital transition - two years of application of the General Data Protection Regulation. COM(2020) 264 final.

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. COM(2022) 68 final.

European Commission 2022b. Commission Staff Working Document: Impact assessment report accompanying the document 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). SWD(2022) 34 final.

European Commission 2022c. Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM/2022/197 final.

European Parliament 2023a. Data Act: MEPs back new rules for fair access to and use of industrial data. Press release, 14 March 2023. Last accessed on 10 May 2023.

European Parliament 2023b. Amendments adopted by the European Parliament on 14 March 2023 on the 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)0068 – C9-0051/2022 – 2022/0047(COD). P9_TA(2023)0069**.**

Ferretti 2022. A single European data space and data act for the digital single market: on datafication and the viability of a PSD2-like access regime for the platform economy. European journal of legal studies, 14(1), 173-218. Last accessed on 10 May 2023.

Graef et al. 2017. Lessons for an Emerging Concept in EU Law. German Law Journal 19 (6), 1359-1398, Tilburg Law School Research Paper No. 2017/22, TILEC Discussion Paper No. 2017-041. Last accessed on 10 May 2023.

Graef 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. Last accessed on 30 June 2023.

Gill and Metzger 2022. Data Access through Data Portability – Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars. European Data Protection Law Review, 3/2022. Last accessed on 10 May 2023.

Hondagneu-Messner 2021. Data Portability: A Guide and a Roadmap. Rutgers Computer & Technology Law Journal, 240. Last accessed on 10 May 2023.

Krämer et al. 2023. Data Act: Towards a balanced EU data regulation. Centre on Regulation in Europe (CERRE). Last accessed on 16 May 2023.

Lindroos-Hovinheimo 2021. Private selves: Legal personhood in European privacy protection. Cambridge University Press, Cambridge.

Meta 2021a. Introducing Meta: A social technology company. 28 October 2021. Last accessed on 10 May 2023.

Meta 2021b. Founder's letter. 28 October 2021. Last accessed on 10 May 2023.

Mäihänniemi 2022a. Attention being bought and sold by online platforms. User's self-determination in governing their own data as a dimension of consumer welfare in antitrust? EU antitrust: Hot topics and next steps: Proceedings of the International Conference held in Prague on January 24–25. Last accessed on 10 May 2023.

Mäihäniemi 2022b. The role of behavioural economics in shaping remedies for Facebook's excessive data gathering. Computer Law & Security Review, 46. Last accessed on 30 June 2023.

Nair et al. 2022. Exploring the Unprecedented Privacy Risks of the Metaverse. ArXiv:2207.13176. Last accessed on 10 May 2023)

OECD 2021. Data portability, interoperability and digital platform competition. OECD Competition Committee Discussion Paper. Last accessed on 10 May 2023.

Pop and Grant 2023. Data portability in the European Health Data Space: Benefits, Risks, and Challenges. EIPA, 29 March 2023. Last accessed on 10 May 2023.

Sitra 2022a. Tracking Digipower: How data can be used for influencing decision-makers and steering the world. Sitra Studies 215. Last accessed on 10 May 2023.

Sitra 2022b. EU regulation builds a fairer data economy: The opportunities of the Big Five proposals for businesses, individuals, and the public sector. Working paper, 7 June 2022. Last accessed on 30 June 2023.

Sitra 2023a. Language evolves: terms of third phase of the internet. Last accessed on 10 May 2023.

Sitra 2023b. Sitra and the Finnish National Gallery's virtual exhibition experiment offered a view of the future art experience. Last accessed on 21 June 2023.

Solove 2023. The Limitations of Privacy Rights. Notre Dame Law Review, GWU Legal Studies Research Paper No. 2022-30, GWU Law School Public Law Research Paper No. 2022-30. Last accessed on 10 May 2023.

Swire 2020. The portability and other required transfers impact assessment: Assessing Competition, Privacy, cybersecurity, and other considerations. Last accessed on 10 May 2023.

Tombal and Graef 2023. The Regulation of Access to Personal and Non-personal Data in the EU: From Bits and Pieces to a System? TILEC Discussion Paper No. 2022-019. Last accessed on 10 May 2023.

Turner et al. 2020. The exercisability of the right to data portability in the emerging internet of things (IOT) environment. New Media & Society, 23(10), 2861–2881. Last accessed on 10 May 2023.

Van Erp 2021. Covid-19 apps, Corona vaccination apps and data "ownership". Last accessed on 10 May 2023.

Wong and Henderson 2019. The right to data portability in practice: Exploring the implications of the technologically neutral GDPR. International Data Privacy Law, 9(3), 173–191. Last accessed on 30 June 2023.

About the author

Sanna Toropainen is a doctoral researcher at the University of Helsinki, affiliated with the Legal Tech Lab. She researches the legal framework for digital identities and the portability of identity-related data via digital identity wallets. She obtained her European law degree (LLB/LLM) from Maastricht University, the Netherlands. Prior to her research, she co-founded a startup to empower individuals to monetise their personal data. Additionally, she has gained in-depth knowledge of privacy and data protection issues through her work as a data protection expert and cyber security specialist in Finland and Belgium. Sitra commissioned Sanna as an external expert to author the memorandum on 'The right to data portability in the fair data economy – Extending the right of individuals to benefit from managing their data'.

SITRA

SITRA MEMORANDUM 6 September 2023
Sitra memorandums are insights produced to support our future-oriented work.

ISBN 978-952-347-348-5 (PDF)
www.sitra.fi

SITRA.FI
Itämerenkatu 11–13
PO Box 160
FI-00181 Helsinki, Finland
Tel: +358 294 618 991