The right to data portability and user control: ambitions and limitations*

Laura Somaini

Abstract

This article covers the right to data portability and analyzes its incidence in relation to the policy objectives set out by the EU regulator. Art. 20 of Regulation (EU) 679/2016 ("GDPR") establishes a general-purpose control mechanism of horizontal application to facilitate the sharing and re-use of personal data among data subjects and promote the free flow of personal data within the European Union. As a key enabler of user control, the right to data portability aims to transform passive subjects into active data re-users. This objective presents an opportunity to develop a user-centric digital environment, by mandating easy retrieval of personal datasets and automatic transfers between digital providers. Nonetheless, the overview of the provision's elements proves that the right applies in a reduced range of situations, suffers several limitations and raises pivotal concerns for data security, undermining the creation of a safe and trust-worthy data-driven environment. Consequently, this article questions the significance of the right's reach and the intensity of the alleged user control, whose beneficial impacts largely depend on the extent to which individuals will exercise the right in practice.

Summary

Keywords

Data portability, Right to data portability, GDPR, Data protection, Personal data

*L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1. Portability: an emerging concept

The portability of data and content is currently emerging as an autonomous new concept in the European framework. The proposed *Directive on certain aspects concerning contracts for the supply of digital content*[1] provides a consumer data retrieval right, with the aim to ensure that consumers benefit from effective protection in relation to the right to terminate a contract. The Portability Regulation[2] seeks to ensure that digital content acquired by consumers in one Member State can be accessed without fee from any other Member State. Such initiatives strive to empower consumers to govern the contractual relationships they conclude online. Furthermore, the EU legislative trilogue reached a provisional political agreement in June 2018 on the proposed *Regulation on free flow of non-personal data*,[3] with the objective to achieve a more competitive and integrated EU market for data storage and processing services. The framework includes a portability principle for professional users, albeit left in practice to industry self-regulation. The proposed regulation, complementing legislation on the protection of personal data, attempts to create a comprehensive and coherent approach to the free flow of all types of data within the European Union. The abovementioned examples demonstrate the relevance and multi-dimensional aspects of portability and data portability in the digital world. The kind of portability this article will focus on is personal data portability, as provided by Art. 20 of the General Data Protection Regulation ("GDPR").[4]

2. Introduction to Art. 20 of GDPR

The General Data Protection Regulation defines data portability as the right of the data subject to obtain personal datasets, «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». The provision encompasses three distinct rights: the right to receive personal data in a structured and machine-readable format, the right to transmit personal data to another data controller and the right to transmit personal data directly from one data controller to another. Art. 20(2) introduces the truly innovative aspect of the right, by establishing a general entitlement to request portable data transfers directly between data controllers, at the choice of the data subject, provided that the transfer is technically feasible. Paragraphs 3 and 4 provide wide balancing clauses for the exercise of

[1] Artt. 13(2)(c) and 16(4)(b) of the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM (2015) 634.

[2] Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168, 30 June 2017, 1–11.

[3] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM (2017) 495.

[4] 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, 4 May 2016, 1–88.

the right, respectively, to protect the exercise of the right of erasure[5] and third-party rights and freedoms.

At the outset, the provision confers an entitlement to natural persons, thus excluding data portability in business-to-business relationships, not covered by the GDPR.[6] The grounds of applicability set by the provision depend preliminary on the compliance of data processing operations with all rules laid down in the GDPR. Accordingly, data subjects must be informed by the data controller about their right to port data in accordance with Artt. 13(2)(b) and 14(2)(c). Pursuant to Art. 20(1)(a), data portability applies where the processing is based either on consent, or on a contract,[7] provided that data processing is carried out by automated means. Conversely, the Regulation does not establish a general right to data portability for circumstances falling outside the abovementioned grounds, as explicitly specified in Recital 68 of GDPR. Furthermore, the right shall not apply where data processing «is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller».[8] In these cases, there is no obligation upon data controllers to provide general data portability.[9]

Although data retrieval and transfer rights are not a new concept and appear straightforward, the discussion *infra* presents contextual, interpretative and technical complexities arising from the new right.

---

[5] This aspect will not be discussed in this article. In short, the European lawmaker did not envisage the exercise of Art. 20 as a tool to simultaneously withdraw data from the original data controller in favor of the receiving controller without exercising the right of erasure. The two rights are founded upon different legal bases and constitute autonomous claims actionable by data subjects. See e.g. P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, in *Computer Law & Security Review*, 34(2), 2018, 10.

[6] Data portability and related rights within B2B relationships are left to arrangements among contracting parties and therefore may vary significantly in a number of given situations. Anecdotal evidence suggests that clauses on data portability are often left out of contracts and that smaller business players encounter difficulties in retrieving their data, for instance, upon termination of the contract. See European Commission, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy*, SWD(2017) 2 final, 47; Id., *Comments made by participants at the EC workshop on Building the European Data Economy*, 21 September 2016.

[7] Regarding the material scope of application of portability, the European legislator's approach is contradictory. Art. 15(3) GDPR on the right of access provides a wider scope, setting out that «the controller shall provide a copy of the personal data undergoing processing» irrespective of the purpose of processing. The EU legislator disregarded the European Data Protection Supervisor's recommendation to provide a wider scope of application for Art. 20. See European Data Protection Supervisor, *Opinion 3/2015 (with addendum) Europe's big opportunity - EDPS recommendations on the EU's options for data protection reform*, 9 October 2015, 12 at fn. 34.

[8] See Recital 68 of GDPR. Where the operation falls under the material scope of application of the right, this may be limited on the basis of the fulfillment of the grounds listed in Art. 23 of GDPR, which aim to protect different facets of public interest sectors. Moreover, Artt. 89(3) and 85(2) provide grounds allowing Member States to place further limitations.

[9] E.g. situations of this kind may be those of financial institutions receiving portability requests concerning personal data processed as part of their obligations under sectorial legislation governing the prevention and detection of money laundering or other financial crimes; or moreover, portability requests concerning professional contact details processed in business-to-business (B2B) relationships in cases where those data are processed on bases other than consent or performance of a contract.

2.1 The setting of data portability: the EU data-driven economy

While data protection law is ever more accused of being «dead letter»,[10] the EU reformed data protection framework ambitiously establishes its dual objective to protect fundamental rights of natural persons and promote the free movement of personal data within the Union, as enshrined in Art. 1(2)-(3) of GDPR. The regulation, remedying previous legislative fragmentation, seeks to strengthen online data protection rights and accordingly, unlock the potential of the digital economy and data-driven technologies. Unjustified restrictions on the free movement of different types of data are likely to constrain the development of the European data economy, impacting the accessibility of more innovative and/or cheaper data services for organizations.[11] Ultimately, this leads to risks of market fragmentation, reduction of the quality of services and of competitiveness of data service providers. In today's context, national boundaries no longer play a dominant role in building barriers to the free flow of data. Rather, these are created by lock-in and data retention strategies implemented by an array of stakeholders. Such obstacles hinder data re-use and sharing and decrease the potential benefits of data.[12]

Raw data has no inherent value in itself.[13] Value can be created where data is contextualized and combined with other datasets in such a way as to produce new insights that become commercially profitable.[14] In this perspective, the metaphor presenting data as «the new oil»[15] is well fitting, in the sense that data, just like oil, in its raw form, is almost useless. Yet, when properly refined, it can be turned into a valuable resource. Therefore, organizations need not merely collect raw data, but rather, they must possess the analytical tools that enable the transformation of data into personality profiles,

[10] B. J. Koops, *The Trouble with European Data Protection Law*, in *International Data Privacy Law*, 4(4) 2014, 258.

[11] The value of the European data economy is expected to increase to €739 billion, 4% of the overall GDP by 2020. See European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy"*, 10 January 2017, COM(2017) 9 final; European Data Market study, SMART 2013/0063, IDC, 2016.

[12] Key barriers to data sharing include: incentives related to upfront investments in data supply, limits to data ownership and control, barriers to data portability and interoperability. Organizational barriers within single organizations in the form of data silos prevent the reuse of data across organizational units. See OECD, *Data-driven Innovation for Growth and Well-being*, Interim Synthesis Report, OECD Publications, 2014, 42.

[13] According to the Financial Times personal data value calculator, the average person's data typically retails for less than one dollar. General information about a person (age, gender and location) is worth a mere $0.0005 per person, whereas a person shopping for a particular product is slightly more valuable to companies promoting those goods. The most expensive troves of data are the most personal and secretive: for $0.26 per person, buyers can access lists of people with specific health conditions or taking certain prescriptions. See Financial Times, *How much is your personal data worth?*, 12 June 2013.

[14] Conseil National du Numérique, *Opinion of the French Digital Council on the Free Flow of Data in the European Union*, April 2017.

[15] The Economist, *The world's most valuable resource is no longer oil, but data*, 6 May 2017. For a critical view, see Harvard Business Review, *Big Data is not the new oil*, 30 November 2012.

in order to adequately tailor products and services.[16] Therefore, the quantity and quality of personal data, as well as the knowledge required to analyze and extract value, are key for successful data-driven businesses.

Whereas data streams typically contain combinations of personal and non-personal information, any policy measure must take into account this economic and contextual reality, while at the same time, ensuring that fundamental rights be respected under the framework on the protection of personal data. Among the instruments that encourage data circulation, create value and develop new uses for data, there are the principle of data portability and tools for data sharing. Respectively, they respond to situations where one actor conducts lock-in strategies and situations where there is necessity to share data between different economic stakeholders.[17]

As data is an essential resource for economic and societal growth, regulating the allocation of data and the ability to control data has become pivotal. The new forms of data sharing and control are key to create genuine value both for economic operators and individuals and generally foster the EU data economy.[18]

2.2 Regulating data portability under data protection law: justification and critique

For the purposes of giving effect to the fundamental right of data protection, Art. 20 of GDPR introduces a new general right to data portability. The GDPR establishes a general-purpose control mechanism of horizontal application, chiefly, to facilitate the sharing and re-use of personal data among data subjects.[19] Before the entry into force of the GDPR, no legal instrument regulated this right in Europe. However, forms of data portability already existed. Typically, certain service providers did provide tools to

[16] See European Data Protection Supervisor, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, 23 September 2016, 6. Indeed, creating value from data is much more a process of cultivation than one of extraction or refinement. The data value cycle describes data-driven innovation processes and includes different phases through which data is transformed: "datification" and data collection (creating a large pool of data, i.e. big data), data analytics (a set of techniques and software tools allowing data to be linked to other datasets in order to be used), the creation of a knowledge base of individuals and organizations accumulated over time through analytics and finally, data-driven decision making. This last phase is what allows to create the social and economic value of data, in the twofold steps of gaining insights, by transforming data into knowledge and taking action, i.e. using it for actual decision making. See OECD, *Data-driven Innovation for Growth and Well-being*, cit., 23.

[17] C. Zolynski, *Free flow of data*, speech at *Digital Assembly 2017*, 16 June 2017.

[18] It should, in principle, benefit online platforms, firms and consumers alike. Applications built on personal data can provide quantifiable benefits of as much as €1 trillion annually by 2020, with one third of the total accruing to private and public organizations, and two thirds accruing to consumers. See Boston Consulting Group, *The value of our digital identity*, Liberty Global Policy Series, 2012. Broadly speaking, data collection and analyzing methods should advantage society, since the knowledge about consumers allows firms to predict future trends and current preferences, a diversity of offers and products will arise, as they may invest in niche products. Furthermore, the use of targeted marketing should reduce the amount of undesirable advertisement and will thus reduce the costs for consumers. See R. H. Weber, *Information at the crossroads of competition and data protection law*, in *Zeitschrift für Wettbewerbsrecht*, 12(2), 2014, 171.

[19] I. Graef - M. Husovec - N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in*

retrieve datasets and established their own terms and conditions to exercise the right.[20] Historically, the debate on data portability arose from the necessity to endow online users with the ability to migrate and share data generated through their online activities. A first market-driven attempt to promote freedom and control over personal data was brought forward in 2007 with the "Bill of Rights for Users of the Social Web",[21] a non-binding document setting out certain fundamental rights for Internet users and duties for website providers. Advocates in favor of portable personal data supported an open approach to ease the migration of users and their data between different websites.[22]

Within the EU legislative discourse, the European Data Protection Supervisor ("EDPS") recommended an express regulation of this right, considering that it would reinforce the set of existing rights of the data subject, in order to «assist individuals in ensuring that providers and other relevant controllers give them access to their personal information while at the same time ensuring that the old providers or other controllers delete that information even if they would like to keep it for their own legitimate purposes».[23] Notwithstanding, the fact that a similar provision has not been experimented before adds on to legal uncertainty and causes serious concerns for addressees of the provision.[24]

From the outset, critics argued that data protection is not the adequate field of law to locate data portability, suggesting that it may be better regulated by consumer protection law;[25] or, as falling within domains that govern abuse of power by commercial

EU Law, Tilburg Law School Research Paper No. 2017/22, 2017, 3.

[20] E.g. Google offers a tool ("Google Takeout"), to download the data created in its own Google+ in a variety of open formats; Facebook offers the feature "Download Your Info". However, in practice, transferring datasets through those functions is anything but an easy procedure, as the data is not extracted in a format that may be easily imported into another social network. Moreover, social network providers do not allow third-party websites to acquire users' data directly. For instance, Facebook prohibits automatic collection of user content, see *Terms of Services on Safety*. For an overview, see S. Sica - V. D'Antonio - G. M. Riccio, *La Nuova Disciplina Europea della Privacy*, Padova, 2016, 236; I. Graef, *Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union*, in *Telecommunications Policy*, 39(6), 2015, 506.

[21] J. Smarr - M. Canter - R. Scoble - M. Arrington *et al.*, *A Bill of Rights for Users of the Social Web*, 2007.

[22] E.g. the Data Portability Workgroup, founded in November 2007. They further argued that data sharing and migration tools could change the economic structure of the web, as businesses rushed to build and enable new services, in order to take advantage of the free circulation of information. See Financial Times, *Social networks may find it does not pay to be too possessive*, 21 January 2008.

[23] See European Data Protection Supervisor, *Opinion on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union",* OJ C 181/01*,* 14 January 2011, 19.

[24] B. Custers - H. Uršič, *Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection*, in *International Data Privacy Law*, 6(1), 2016, 1; O. Lynskey, *Aligning data protection rights with competition law remedies? The GDPR right to data portability*, in *European Law Review*, 42(6), 2017, 794.

[25] This criticism was pointed out in a reservation made by the UK within the Council of the EU. Several other delegations also remarked that data portability could be a rule of competition law and/or intellectual property law. See *Note from the Presidency of the Council of the European Union to the Working Group on Information Exchange and Data Protection (DAPIX) on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 7978/1/15 REV 1, Brussels, 12 May 2015, 45. The relevance of data portability within the consumer protection framework is supported by the

operators, under the scope of unfair business practices and electronic commerce legislation, or moreover, in the ambit of competition law.[26]

Framing such power abuse under questions of data protection law, the argument would continue, may lead to introducing new types of protection into an already complex system. Along these lines, in 2014 the European Data Protection Supervisor introduced, conveniently, a debate on the interplay between data protection, consumer protection and competition laws in the framework of the digital economy.[27] Indeed, in data-driven consumer markets, the boundaries of consumer and data protection laws are not undisputed. The two areas of law have progressively drawn closer on data-related issues, at EU legislative and policy-making level. Notwithstanding, personal data exercise a critical role and must be clearly framed to ensure adequate protection.[28]

In practice, the right was successfully negotiated within the Council of the European Union and as the GDPR has entered into force, *de lege lata* data portability falls within

case of French law *Loi no. 2016-1321 du 7 octobre 2016 pour une République numérique*. The revised French Consumer Code *Loi No. 93-949 du 26 Juillet 1993* now provides a new right of consumer data portability for all types of data applicable to providers of online public communications services.

[26] B. J. Koops, *op. cit.*, 14; O. Tene - J. Polonetsky, *Big data for all: Privacy and user control in the age of analytics*, in *Northwestern Journal of Technology and Intellectual Property*, 11(5), 2013, 269. At the time of the proposal for the GDPR, then-Commissioner for Competition Almunia stated that «only time will tell» whether the right qualified as a matter for regulation or competition policy. J. Almunia, *Competition and personal data protection*, speech at Privacy Platform, *Competition and Privacy in Markets of Data*, Brussels, 26 November 2012. It cannot be excluded that the European Commission may enforce competition rules where a dominant provider impairs users' ability to port personal data when switching online services. See also D. Geradin - M. Kuschewsky, *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue*, in *SSRN Electronic Journal*, 2013, 13. Indeed, the fact that the Commission has taken action towards enabling the transfer of professional user data, within the Google investigation IP/10/1624 initiated in 2010 regarding the limitation of portability of advertising campaign data, supports the possibility to consider portability also as a competition issue.

[27] European Data Protection Supervisor, *Preliminary Opinion on the Privacy and Competitiveness in the Age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014. In 2017 the EDPS also established the Big Data & Digital Clearing House, endorsed by resolutions of the European Parliament (14 March 2017) and of the 2017 International Conference of Privacy and Data Protection Commissioners. The Digital Clearing House aims to bring together agencies from the areas of competition, consumer and data protection laws willing to share information and discuss how to enforce rules in the interests of the individual in the most effective way.

[28] Different approaches could be devised. One approach supports a strict division of tasks between the two fields, where all matters related to personal data fall primarily under data protection law. However, a drawback may be that data protection would cover increasingly greater aspects regarding digital markets. Growing criticism argues that data protection law, by setting informed consent as the paramount legal basis for data processing in consumer transactions, does not afford an optimal level of protection of the interests of online consumers. A second approach endorses parallel applicability of consumer and data protection laws. Ideally, along these lines, the two fields of law would complement each other and offer a comprehensive set of rights and remedies to provide a high level of protection in the digital market ecosystem, be individuals vested in their capacity as consumers or as data subjects. However, the interplay between the areas of consumer and data protection is not yet sufficiently well understood. See See N. Helberger - F. Zuiderveen Borgesius - A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, in *Common Market Law Review*, 54(5), 2017, 1428-1429; B. J. Koops, *op. cit*. Broadly speaking, there is a need to develop a sophisticated integrated approach of the relevant provisions in competition, consumer, data protection and intellectual property laws, to foster a well-functioning framework for the protection of privacy in the digital economy. See W. Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*, in *Journal of Intellectual Property Law & Practice*, 11(11), 2016, 866.

the scope of data protection law and must be treated accordingly.[29]

3. Policy objectives of the right to data portability

At its heart, data portability essentially constitutes the ability for individuals to re-use their data across interoperable applications. Whilst the broader goal is to foster the free development of the human personality, the means to do so are technical processes directly connected to the protection of informational privacy on the one hand, and ensuring a level playing field among digital service providers, on the other.[30] Within the EU legal framework, the right to data portability is devised along the human rights rationale underlying EU data protection law.[31]

Firstly, a general data portability right allows the individual to enjoy a strengthened right to informational self-determination,[32] overarching objective of the data protec-

[29] The Article 29 Working Party rightly points out that: «the GDPR is regulating personal data and not competition». See Article 29 Working Party, *Guidelines on the right to data portability*, WP 242, rev.01, 5 April 2017, 4. See also European Data Protection Supervisor, *Privacy and competitiveness in the age of big data*, cit., 32. The European Commission clearly held that data portability falls within the scope of data protection, as a means to enhance the free flow of data within the Union. See e.g. N. Dubois, Policy Officer Data Protection Unit at DG Justice, *Data Portability at the crossroads of data protection and competition policy*, speech at BITS Seminar on Data Portability, Brussels, 29 April 2014.

[30] The idea associating data portability to the human personality derives from the concept of a "digital identity", where personal data and their combination may be interpreted as a continuation of one's personality in the digital environment. See G. Zanfir, *The right to Data portability in the context of the EU data protection reform*, in *International Data Privacy Law*, 2(3), 2012, 3. On the other hand, data portability aims to tackle specific problems of technology market scenarios. According to Van der Sloot, Art. 20 of GDPR was specifically designed to break Facebook's dominance in the data economy. See B. van der Sloot, *Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation*, in *International Data Privacy Law*, 4(4), 2014, 319.

[31] Albeit not mentioned expressly in Art. 8 of the EU Charter of Fundamental Rights, the right to data portability constitutes a facet of the right to data protection, in accordance with the legislative history of the GDPR. Contemplating data portability as a fundamental right, as part of the jurisprudence on data protection in the EU, is underpinned by the goals of the Regulation itself, pursuant to Art. 1. Furthermore, the European Commission holds that «not being able to use these media [Web 2.0 tools and social media] effectively restricts the exercise of fundamental rights in the social reality». See European Commission, *Commission Staff Working Paper Impact Assessment*, 29 SEC(2012) 72 final. However, doubt on its status as a fundamental right was cast by part of scholarship. See P. Swire - Y. Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, in *Maryland Law Review*, 72(2), 2013, 339. A non-fundamental dimension is supported by the instrument's legal basis, Art. 16 of TFEU, mandating the use of the ordinary legislative procedure. Nevertheless, the EU Charter does not create a hierarchy of rights. The Court of Justice, in CJEU, C-293/12, *Digital Rights Ireland* (2014), at para 40, supported that further data protection rights may fall within the scope of Art. 8. Although interpreting the Charter in light of secondary legislation may constitute a logical fallacy, the approach of the Court suggests that there should be no preclusion to a fundamental standing of the right. Nonetheless, the precise relationship between the objectives and implications of Art. 20 of GDPR remains contested. If it is recognized a fundamental right status, the right to data portability should be able to trump competing economic interests, as the Court maintained in CJEU, C-131/12, *Google Spain* (2014), at para 97, that Artt. 7 and 8 of the Charter «override, as a rule» economic interests of data controllers in the context of the legitimate interests test. See O. Lynskey, *Aligning data protection rights with competition law remedies? The GDPR right to data portability*, cit., 794, 812.

[32] See e.g., G. Zanfir, *op. cit.*; E. Fialova, *Data Portability and Informational Self-Determination*, in *Masaryk University Journal of Law and Technology*, 8(1), 2014, 47-48; G. Finocchiaro, *Il nuovo Regolamento europeo sulla*

tion reform. In this context, the availability of workable mechanisms for data subjects to access, modify, delete, transfer, or otherwise further process (or let third parties process) their own data will result in empowering data subjects,[33] allowing them to benefit from value-added services of third parties and "share the wealth" created by big data.[34] Effective data control is an important precondition to ensure that individuals enjoy a high level of data protection.[35] As stated in the opening sentence of Recital 68 of GDPR, the new right aims to strengthen individual control of data subjects over their own personal data and hence, sits coherently within the renewed data protection regime.[36] For the purposes of EU data protection law, user control ensures that individuals be empowered to detect unfair biases and challenge mistakes more easily and effectively and helps prevent secondary uses of data for purposes that go beyond legitimate expectations of the data subject.[37] The European Data Protection Supervisor described the right as «allowing the individual to decide what happens to their data».[38] It allows individuals to self-present: by providing greater control over data, different elements of their personality can be revealed to different audiences instead of a "one size fits all" disclosure deriving from a lack of data control.[39] Through user control, the right seeks to transform individuals from passive subjects into active data re-users within an interconnected digital environment, beyond mere data accessibility.[40] The right aims to achieve full accessibility, easy management and re-usability of personal data. This specificity relies on the requirement that data processing and transmission

privacy e sulla protezione dei dati personali, in *Le riforme del diritto italiano*, Bologna, 2017, 6.

[33] Empowerment in this context encompasses the individual's perception of the extent to which he or she can control the dissemination and use of his or her personal information. See V. Midha, *Impact of consumer empowerment on online trust: An examination across genders*, in *Decision Support Systems*, 54(1), 2012, 198-205.

[34] Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, 2 April 2013, WP203, 47. See also P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 11.

[35] European Commission, *A comprehensive approach on personal data protection in the European Union*, 2010, COM(2010) 609 final, 7; *Id.*, *Impact Assessment*, cit.; European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability, 19 November 2015,* 5. See also S. Sica - V. D'Antonio - G. M. Riccio, *op. cit.*, 237.

[36] Individual control over personal data constitutes an autonomous normative objective underpinning the EU data protection framework, thus justifying the coherence of Art. 20. See Recital 7 of GDPR; O. Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, cit., 809. Within the setting of the GDPR policy objectives, data portability is devised as an operational objective within the specific objective of individual control over personal data and trust in the digital environment. The latter is, in turn, specific to the general objective to increase the effectiveness of the fundamental right to data protection. Data portability should reduce "grey areas" where rights of individuals are not properly respected. See European Commission, *Impact Assessment*, cit., 43, 67.

[37] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, cit., 5; Id., *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, 15 December 2015, 4.

[38] European Data Protection Supervisor, speech at *Brussels Matters*, Brussels, 21 May 2015, 5. The EDPS mentions «true data portability» as capable of bringing about a paradigm shift in the digital revolution.

[39] O. Lynskey, *Deconstructing Data Protection: The 'Added-Value' Of A Right To Data Protection In The EU Legal Order*, in *International and Comparative Law Quarterly*, 63(3), 2014, 591.

[40] B. Custers - H. Uršič, *op. cit.*

should be executed in formats that support re-usability, with little or no effort by the data subject. The rationale is thus directly linked to the principle of data quality, which ensures the "useableness" of datasets.[41]

Secondly, the provision aims to correct a common situation characterizing data-driven markets, where data retention serves as an obstacle for online users to freely choose services.[42] Within this context, a switching cost occurs where users are effectively impeded from changing services, regardless of the fact that better, cheaper or more "privacy-friendly" services become available on the market.[43] As services are tailored to individuals based on their data, the information upon which specific adjustments are perfected becomes extremely valuable in terms of commercial profitability. Data portability is generally associated with low switching costs and low market entry barriers,[44] therefore, if properly implemented and enforced, the general right should mitigate the reluctance of users to give up profiles and sets of information created over time.[45] Therefore, the easier it is for a data subject to transfer personal data from an online service to another, the easier it will be to switch from one provider to another, while continuing, at the same time, to benefit from customized adjustments.[46]

Thirdly, the entitlement to request the transfer of personal datasets eases the process to move, copy or transmit personal data from one IT environment to another.[47] In this sense, data portability constitutes data re-use *per se*.[48] Data portability should help

---

41 For the definition of "qualitative dataset", see Open Data Handbook, *Glossary*.

42 According to a Eurobarometer survey of 2011 on data protection in the EU, 71% of respondents claimed that the ability to transfer personal information stored and collected through a website when changing service provider or quitting the service was important to them. Furthermore, social networking or sharing website users (both 75%) resulted more likely to value the portability of personal data than those not involved in activities of the social web (both 67%). See European Commission, *Data Protection and Electronic Identity in the EU*, Special Eurobarometer 359, 2011, 160-161.

43 European Commission, *Impact Assessment*, cit., 28; see also S. Sica - V. D'Antonio - G. M. Riccio, *op. cit.*, 235-236. Specifically, this may entail the loss of contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially significant data, in turn, very difficult to recreate or restore. Even where possible, re-entering data manually may constitute a major effort. Moreover, switching costs may prevent consumers from using various services, i.e. multi-homing, in equal proportions. In case of price increases or changes in services, users have a reduced negotiation power. See B. Engels, *Data portability among online platforms*, in *Internet Policy Review*, 5(2), 2016, 2. As data portability and switching of service providers are mutually dependent, the Commission is favorable to the development of standard contract terms requiring the service provider to implement the portability of users' data. See European Commission, *Building a European Data Economy*, cit., 16.

44 European Commission, *Building A European Data Economy*, cit. See also W. Kerber - H. Schweitzer, *Interoperability in the digital economy*, Joint Discussion Paper Series in Economics, MAGKS, 12, 2017, 20. In fact, switching costs are negatively correlated with data portability, i.e.: the easier it is for users to port their data from one platform to another, the lower will costs to switch to another platform be. See B. Engels, *op. cit.*, 3.

45 European Data Protection Supervisor, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, cit., 14. The Article 29 Working Party held that the right to portability would put «a clear end» to user lock-in situations. See Article 29 Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things*, WP 223, adopted on 16 September 2014, 20; S. Sica - V. D'Antonio - G. M. Riccio, *op. cit.*, 240.

46 K. Coates, *Competition Law and Regulation of Technology Markets*, Oxford, 2011, 405.

47 Article 29 Working Party, *Guidelines on the right to data portability*, cit., 4.

48 B. Custers - H. Uršič, *op. cit.*

rebalance the relationship between data controllers and data subjects, jeopardized by substantial power and information asymmetries. Indeed, safeguards allowing direct access to one's datasets in a portable, user-friendly and machine-readable format may redress economic imbalances,[49] even more so where the data subject is entitled to request direct data transfers between controllers. Adopting this approach entails a more fair and transparent involvement of individuals, supporting, on the other hand, the minimization of unfair or discriminatory practices and reduction of risks linked to uses of inaccurate data for decision-making purposes.[50]

Fourthly, data portability constitutes a feature to promote competition in those markets that require consumers to take their data when changing service provider.[51] It should, therefore, serve as an incentive for controllers to improve services, in order to retain their customer/user base because of the high value of the service itself, rather than relying on poor data protection conditions that lock consumers into their services or platforms.

Fifthly, data portability is expected to promote data-driven innovation within the digital single market, by incentivizing developers of digital services to offer additional features and applications to the benefit of users.[52] In fact, obstacles impeding data re-use and sharing may lead to stifle benefits deriving from potential unexpected uses. Data portability is a tool for data circulation, value creation and should drive the development of new uses for personal data in the digital environment, in a safe and secure manner, under the control of an informed data subject.[53] Likewise, data portability should promote a controlled data sharing between organizations and thus, help enrich services and customer experiences online.

Data portability, therefore, as part of the rationale of data protection legislation, enshrines a double objective: an economic and a human rights objective. It endows data subjects, as recipients of both general and specific positive obligations, with control and freedom over their online consumerist choices. As a result, the general right to data portability is instrumental to support the free flow of personal data within a level playing field for data controllers.[54] In theory, the provision constitutes a valuable attempt to attain effective data control, genuine freedom of choice online and the ability

[49] Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, cit., 47; European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, cit., 13.

[50] Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, cit., 47; P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 2.

[51] J. Almunia, *op. cit.* The former Commissioner for Competition explicitly stated: «customers should not be locked in to a particular company just because they once trusted them with their content». See also D. Geradin - M. Kuschewsky, *op. cit.*, 11.

[52] P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 2; International Working Group on Data Protection in Telecommunications, *Privacy principles under pressure in the age of Big Data analytics*, Working Paper on Big Data and Privacy, 55th Meeting, Skopje, 5-6 May 2014, 16. The International Working Group suggests that data portability, over time, should foster more privacy-friendly services.

[53] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 5.

[54] European Data Protection Supervisor, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, cit., 3.

to make better-informed and safer choices regarding the use of data.

3.1 Reality and risks of user control

As discussed, the EU legislator devised a general right to data portability pursuing multifold objectives. The discussion will focus on the primary objective of the right under data protection law, i.e. achieving control over personal data. This section casts doubt on the significance of user control and displays the risks that data portability could produce.

The rhetoric of data control has been a building block of the data protection reform and the rationale of the right to data portability. Indeed, the idea of empowering individuals to reclaim their data, by suggesting that personal data "belong" to the data subject, is widespread in Europe and internationally.[55] Arguments claiming property-related features of data portability,[56] relying on the right's potential to enable the data subject's entitlement to trade data and to "take their data and leave", should be nuanced. As it is, the right does not produce the key characteristic of property, i.e., the right to exclude.[57] To the contrary, data portability promotes data circulation and sharing. In time, the concept of data portability could foster the idea that personal data, rather than amounting to an asset exclusively held by either individuals or organizations, may be instead treated as a joint resource and a basis for innovation and value

[55] See e.g., European Data Protection Supervisor, *Towards a new reality: Taking back control of our online identities*, Press Release, Brussels, 20 October 2016; J. Brill, *Reclaim Your Name*, Keynote speech at *23rd Computers Freedom and Privacy Conference*, Federal Trade Commission, Washington DC, 26 June 2013.

[56] See e.g., I. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law,* 3(2), 2013, 5, 8; D. Geradin - M. Kuschewsky, *op. cit.*, 10; P. Swire, *The Right to Data Portability: Privacy and Antitrust Analysis*, George Mason Conference on Search & Social Media, 16 May 2012. Prof. De Hert argues that data portability constitutes a «first step» towards the idea of default ownership over personal data. See P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 9. The possibility that the rationale of the right may amount to individual ownership is also suggested in B. van der Sloot, *op. cit.*, 315. In this context, data portability is often compared with number portability, where Directive 2002/22/EC ("Universal Service Directive") created a *quasi*-property right over mobile telephone numbers. Number portability was designed to reallocate entitlements from economic operators to consumers and ensure that consumers be able to change their provider while maintaining their original number. The rationale lies with the expectation of eliminating (or at least reducing) costs for switching, thereby making the sector more competitive. See e.g., S. Buehler - R. Dewenter - J. Haucap, *Mobile number portability in Europe*, in *Telecommunications Policy*, 30(7), 2006. Although the two provisions are often compared and share the entitlement to request a service provider to transmit a dataset or number directly to a new provider, they do not overlap. Firstly, the way in which the requirement to transfer is framed is different: the GDPR awards a general right under certain circumstances, whereas in the telecommunications framework, a general duty to enable number portability is imposed on all providers. Secondly, the policy objectives differ: the GDPR promotes data protection rights, whereas the Universal Service Directive sought to foster competition in the telecom sector. Thirdly, whereas telecom operators merely allocate to their customers a number assigned by a public authority, Art. 20 of GDPR does not confer ownership over ported data but merely facilitates control for the purposes of re-use. Contrary to a mere issue of technology, the data portability framework may have far-reaching effects and results in additional complexities due to the nature of their object, i.e. personal data, requiring adequate remedies. See I. Graef, *Mandating portability and interoperability in online social networks*, cit., 504, 506, 508, 512.

[57] I. Graef - M. Husovec - N. Purtova, *op. cit.*, 6-7. In general, data are non-rival and non-exclusive, as no contract prevents users from sharing their personal information with multiple parties.

creation.[58]

In practice, the perception of control over personal data in the European Union is very low, where only 15% of users claim they have «complete control»; conversely, some 31% of users perceive «no control at all» over their personal information.[59] A similar assessment was remarked by the Article 29 Working Party ("WP29"), with regards to decisions made by complex technological systems, where it found that individuals «do not understand and have no control over» such decisions.[60] This apparent trust crisis is attributable to the inconsistency of purposes for which personal data are used and a significant difficulty to hold service providers accountable.[61] Indeed, in data-driven environments, data collected by a service provider will likely be shared with and used by other entities along the value chain. Individuals do not merely enter into a bilateral relationship with their original provider, but rather in a multilateral one with numerous entities whose uses of those data may be opaque, or unknown.

Critical arguments point out that EU data protection law relies too heavily on informational self-determination and wrongly places the focus on user empowerment.[62] In theory, data protection law attempts to correct internal failings that prevent individuals from controlling their personal information in an effective manner.[63] It provides individuals with actionable tools to avoid being *de facto* locked into contractual relationships concluded online, such as consent, rights to information, rights of access, portability, rectification and deletion of data. However, individual control is inherently frustrated by information and power asymmetries between individuals and organizations.[64] Such asymmetries are created by an imbalance in the amount and quality of information about individuals held by, or accessible to, industry and governments, combined with individuals' inability to govern the use of their own data.[65] Along these lines, individual

[58] O. Tene - J. Polonetsky, *op. cit.*, 269.

[59] The remaining 50% of surveyed respondents perceive «partial control» over their personal data. Of the respondents perceiving they do not have complete control, 67% claims to be concerned by the issue. See European Commission, *Data Protection*, Special Eurobarometer 431, 2015, 9.

[60] Article 29 Working Party, *Opinion 3/2013 on Purpose Limitation*, cit., 45. See also S. Sica - V. D'Antonio - G. M. Riccio, *op. cit.*, 227.

[61] A high level of trust is essential for attaining the data-driven economy. See European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Towards A Thriving Data-Driven Economy*, COM(2014) 442 final. In turn, trust requires the essential prerequisites of legitimacy and effectiveness, necessary to regain and ensure that citizens trust the Union's ability to deliver in the areas of data protection and privacy. For an overview, see H. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, in *Law, Governance and Technology Series* 31, Dordrecht - Heidelberg - London - New York, 2016, 5-6.

[62] See B. J. Koops, *op. cit.*, 251-253.

[63] F. Costa-Cabral - O. Lynskey, *Family Ties: the intersection between data protection and competition in EU law,* in *Common Market Law Review*, 54(1), 2017, 19.

[64] C. Lazaro - D. Le Métayer, *The control over personal data: True remedy or fairy tale?,* in *Scripted. A Journal of Law, Technology and Society*, 12(1), 2015, 3; for a critical argument, see R. Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in S. Gutwirth - Y. Poullet - P. De Hert, *et. al.* (eds.), *Reinventing Data Protection*, Dordrecht - Heidelberg - London - New York, 2009, 83-109.

[65] World Economic Forum, *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems*, Industry Agenda, May 2014, 3.

control constitutes an insurmountable fallacy, unlikely of ever being achieved.[66] Furthermore, the newly established user control tool could also foreshadow risks for security and individual privacy. A lack of security undermines user confidence and trust towards particular services and the general functioning of the market.[67] Data access and openness inevitably produces tensions with the principle of data security. While controllers must ensure that the data they hold is appropriately secured, mandatory portability, nonetheless, poses threats of breaches in the course of data transmission and may create significant tension with the right to data security.[68] System interoperability, on which portability relies, may also magnify this problem, as a factor increasing security and privacy breaches and potential fall-outs.[69] Allegedly, data portability could even cause a «race to the bottom on privacy»,[70] for instance, where data controllers do not ensure equivalent levels of data protection. Personal data could be used wrongfully, e.g. to scrap information from third-party websites and in such cases, the harms may well be worse than those of the restriction of portability.[71] The proliferation of openly accessible data access points, whether in the form of export functionalities or application programming interfaces ("API"), increases the risk of data security breach-

[66] In other words, «the delusion that data protection law can give individuals control over their personal data, which it cannot». B. J. Koops, *op. cit.*, 251-253. Part of scholarship also holds that individual control over personal data in certain contexts, namely, where individuals face monopolies, is simply «illusionary». See C. Kuner - F. H. Cate - C. Millard - D. J. B. Svantesson - O. Lynskey, *When two worlds collide: the interface between competition law and data protection*, in *International Data Privacy Law*, 4(4), 2014, 247. Broadly speaking, research has shown that the main concerns in the field of privacy and social network applications are related to the inability of users to maintain control over the transfer of personal information and the lack of transparency of the process. See B. Van der Auwermeulen, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, in *Computer Law and Security Review*, 33(1), 2017, 60.

[67] See e.g., Recitals 1 and 2 of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 July 2016, 1-30. The Digital Single Market Strategy pursues as a priority the reinforcement of trust and security in digital services and in the handling of personal data in the context of the digital single market. See European Commission, *Communication A Digital Single Market Strategy for Europe*, 6 May 2015, COM(2015) 192 final, pt. 3.4.

[68] The principle of data security is enshrined in Art. 32 GDPR as a reflection of the duty on data controllers to ensure security of data processing and Art. 40(2)(h) provides the preparation of codes of conduct for security measures. The definition of the right to data portability should be completed in full awareness of these risks; however, there is no mention of it in the plain text of Art. 20, Recital 68, nor in the WP29's Guidelines. See P. Swire - Y. Lagos, *op. cit.*, 373. For an overview, see F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, *Il Regolamento europeo 2016/679*, in *I diritti nella "rete" della rete*, Torino, 2016, 289.

[69] U. Gasser, *Interoperability in the digital ecosystem*, Berkman Center Research Publication No. 2015-13, 2015, 13-14.

[70] J. Grimmelmann, *Saving Facebook*, in *Iowa Law Review*, 94(4), 2009, 1194. Indeed, complete data portability may have an adverse impact on data protection, because a ported dataset into a receiving online platform may not provide an equivalent degree of protection. See R. H. Weber, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, in *Concorrenza e Mercato*, 23(59), 2016, 68; Id., *Information at the crossroads of competition and data protection law*, cit., 179; F. Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, in *Northwestern University Law Review*, 104(1), 2010, 153 at fn. 256. In the context of social networks, «once data becomes completely portable, people can easily evade any privacy restrictions placed by the initial social networking site simply by porting the data over to another venue not subject to those restrictions». See C. S. Yoo, *When Antitrust met Facebook*, in *George Mason Law Review*, 19(5), 2012, 1155.

[71] R. H. Weber, *Information at the crossroads of competition and data protection law*, cit., 179.

es.[72] The Article 29 Working Party identifies twofold aspects for the data controller's responsibility. On the one hand, the transmission process itself requires important measures to guarantee its integrity (by using, e.g., data or end-to-end encryption). On the other, the controller must also assure that the data is transmitted to the correct recipient (for instance, applying strong authentication measures).[73] Notwithstanding these concerns, Art. 20 is designed to allow to download and receive, at once, a lifetime worth of personal information, with the additional requirement for controllers to comply «without hindrance».[74] The WP29 recommends that data controllers assess specific risks linked with data portability and take appropriate measures to mitigate those risks.[75] Further concerns, not explicitly addressed by the WP29, include the allocation of responsibilities in the case of a direct transfer between data controllers, where the original transmitting controller is not able to verify the receiving controller, even where designated by the data subject.[76] Viable security norms and standards must be developed and arguably, data controllers should be able to legitimately reject portability requests in the interest of the data subject. Finally, another concern lies within the responsibility of the data subject: namely, the risk that storage facilities, systems and devices used by individuals do not meet adequate – or even minimum – standards

[72] P. Przemysław Polański, *Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal*, in *Journal of European Consumer and Market Law*, 7(4), 2018, 145-146. For instance, Facebook has many APIs (e. g. Facebook Login API, Pages API, Groups API etc.) with multiple entry points, which enable software developers to obtain access to personal data. Improperly implemented APIs could lead to massive data security breaches through loopholes found in popular web frameworks and result in the proliferation of harmful content in cyberspace.

[73] Article 29 Working Party, *Guidelines on the right to data portability,* cit., 19. The GDPR addresses the issue linked to authentication in Art. 11(2), where the data subject may provide further information to allow identification, while Art. 12(6) enables data controllers to request further information where they have reasonable doubts concerning the data subject's identity. See O. Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, cit., 808. However, the recommendation of technical safeguards does not take into account the additional burden of developing such tools for the data controller, nor does it provide an acceptable standard of encryption to meet the legal obligation of security. See Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability*, cit., 14.

[74] Indeed, this should not be interpreted as prohibiting an online provider from acting upon signals of a higher risk of identity fraud, such as double checking the identity of the subject issuing a portability request, for instance, when the request comes from a new IP address. See P. Swire - Y. Lagos, *op. cit.*, 374-375.

[75] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 19. Examples of what those measures may include: additional authentication information (e.g. shared secret or one-time passwords), suspension or freezing of the data transfer where there is suspicion that an account has been compromised, authentication by mandate (e.g. token-based authentication). However, the WP29 points out that these measures cannot prevent data subjects from exercising their rights, nor should they impose additional costs on the data subject. For an overview of recommendations on technical and organizational measures, see Article 29 Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 3 October 2017, WP250, 5-6; for a business perspective, see C. Tankard, *What the GDPR means for businesses*, in *Network Security*, 6, 2016, 7-8. It may be plausible for data protection authorities to regulate this matter, fulfilling the task referred in Art. 57(i)(v) of GDPR. The effort may also be met at EU level through the consistency mechanism in accordance with Art. 64(2) of GDPR. See L. Scudiero, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability Reports: Practitioner's Corner*, in *European Data Protection Law Review*, 3(1), 2017, 124-125.

[76] Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability*, cit., 14.

of security. Informational education is still limited, yet, a necessary step to achieve empowerment and meaningful data control.
In practice, the ability of the right to positively enhance user control depends on the willingness and the extent to which data subjects will actually exercise their rights, hold data controllers accountable and demand that high security standards be respected in order to foster a safe and trust-worthy data environment.

4. Overview of the elements of Art. 20 GDPR

This paragraph presents the elements of the general right to data portability. Through the analysis of its features, the discussion demonstrates that Art. 20 applies in a reduced range of situations and suffers substantial limitations, putting into perspective the ambitions of the right and its ability to bring about a paradigm shift in the data-driven economy.

4.1 The right to receive personal datasets: Art. 20(1)

Firstly, Art. 20 endows the data subject with a right to receive personal data provided to and processed by the data controller and to further store that data for any other use. In this dimension, the right resembles a comprehensive form of access, pursuant to Art. 15 of GDPR. However, the Regulation is silent as to what kinds of uses follow from ported data. Art. 20 provides no specification as to the data processing method in order to exercise the right, insofar as the processing is carried out by automated means, pursuant to Art. 20(1)(b), therefore, slightly restricting the material scope of the GDPR.[77] The formats that the data subject receives shall be «structured, commonly used and machine-readable», despite the processing method used by the data controller. This feature of the right requires data controllers to implement export and download functionalities to enable transmission in a structured and machine-readable format,[78] chiefly, to allow re-usability.
The provision in force removes the discriminatory applicability that was initially pro-

[77] As noted, the GDPR regime applies to processing «wholly or partly by automated means […]» as per Art. 2(1). Data portability, conversely, may be exercised in the circumstances of processing executed «wholly» by automated means. Nevertheless, it seems likely that Art. 20(1) will be interpreted in light of Art. 2(1) GDPR, thus including also «partly» automated processes, given that attempts to narrow the scope of data protection legislation through an excessively restrictive interpretation of the automation criterion have been overlooked by the Court of Justice in the past. See Opinion of AG Sharpston in C-28/08, *Commission v Bavarian Lager* (2010); discussed in O. Lynskey, *Aligning data protection rights with competition law remedies? The GDPR right to data portability*, cit., 800.

[78] The term "machine-readable" refers to data in a format that may be automatically read and processed by a computer, where the representation of the data on disk does not represent the actual relationships present in the data (formats of the kind are, e.g., CSV, JSON, XML). This entails that computer programs should be able to process incoming data automatically, with no or minimum human involvement. See Open Data Handbook, *Glossary*, cit.

vided in the Draft Regulation,[79] which limited informational self-determination of those subjects whose personal data was processed electronically but in untraditional formats.[80]

The provision further declines the right by imposing an obligation as to the modality of performance, i.e. «without hindrance». The requirement indicates that the data controller must ensure the absence of any legal, technical or financial obstacle, refraining or slowing down the access, transmission or re-use of portable datasets to the expense of the data subject or the receiving controller. By way of example, fees for data delivery, lack of interoperability or access to a data format or APIs, or the provided format, as well as excessive delay or complexities to retrieve the full dataset, deliberate obfuscation of the dataset, specific and undue or excessive sectorial standardization or accreditation demands, may generally be considered as constituting «hindrance».[81] Nevertheless, legitimate obstacles may justify hindrance in the execution of portability requests, for instance, where the data controller is not able to identify the data subject. In such cases, the burden of providing justifications as to why an obstacle may be legitimate lies with the data controller. Although it is not undisputedly clear what may constitute hindrance in the handling of portability requests, insofar as time constraints, or excessive delays are involved, the limits provided by Art. 12 of GDPR, apply.

4.2 The right to transmit datasets directly between data controllers: Art. 20(2)

Art. 20(2) of GDPR provides the data subject with the right to request that their personal data be ported directly to another controller of their choice. This "controller-to-controller" data portability is far more significant than the individual's right to merely retrieve or transfer data. The provision establishes a general-purpose mandate addressed to data controllers to carry out automatic transfers to other providers,[82] re-

[79] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final.

[80] Art. 18(1) of the Draft Regulation provided a right for the data subject to obtain from the data controller a «copy» of data undergoing processing, provided that his or her data were processed by electronic means and in a structured and commonly used format. Although a majority of data processing is electronic, the Draft Regulation did not entitle the data subject to choose the format of processing, nor did it require that the data subject be informed about what format would be used. This subtle distinction could have resulted in a disadvantage upon one group of data subjects, namely, those whose personal data were not processed by electronic means, or not in a structured and commonly used format - essentially depleting their ability to exercise the right. It may also have encouraged controllers to avoid the use of structured and commonly used formats, either to spare the costs of copying and transmitting datasets or to impede the migration of data subjects to other services. See E. Fialova, *op. cit.*, 48-51, 54.

[81] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 15.

[82] According to the Commission's Proposal, the legal base for exercising the right was different whether the individual requested to receive a copy of his/her personal data or to transmit the dataset to another controller. In the first case, the proposed Art. 18(1) did not specify the legal basis, consequently allowing applicability of the general GDPR legal basis; whereas in the second case, paragraph 2 specified that the direct data transfer between data controllers was applicable insofar as the data was provided by the subject and where the processing was based on consent or contract.

gardless of the business sector involved. This innovative feature is oriented towards the interconnection of digital services.[83] Controlled data sharing between providers should be promoted with the view of enriching available services and improving consumer experiences.

Nonetheless, the provision restricts the scope of direct portability when such operations are «technically feasible». The GDPR does not clarify what circumstances determine technical feasibility and may result in creating undue leeway to bypass the provision.[84]

The Regulation prohibits data controllers from construing and establishing barriers hindering seamless data transmissions. Accordingly, data controllers should facilitate the exercise of data subject rights, pursuant to Art. 12(2), within the context of transparent modalities for the exercise of the rights of data subjects. On the other hand, data controllers may incur in significant costs and efforts to comply with data transfer requests. Controller-to-controller portability requires a digital service provider to write specialized code in order to export data from the sending service's system and import it to another recipient system.[85] On the one hand, the Article 29 Working Party suggests that implementation costs of Art. 20 are encompassed in ordinary business costs and the European Commission maintained that those costs are minimal, since the transfer of user data is usually already possible through other interfaces, e.g. for third-party application developers or exchanges with affiliated companies.[86] On the other hand, industry and scholars note that this requirement may result in disproportionate costs for smaller organizations, as they may not possess the resources to fully understand and implement the technical procedures for direct data transfers.[87]

---

[83] P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 4.

[84] A. Diker Vanberg - M. B. Ünver, *The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*, in *European Journal of Law and Technology*, 8(1), 2017, 3.

[85] P. Swire - Y. Lagos, *op. cit.*, 344-45. According to a broad reading of the right, the export-import code, likewise other technical services, are needed to ensure that data exportation from one controller and importation into the system of another controller, be carried out «without hindrance», as per Art. 20(1) of GDPR. This requirement supports a strong form of interoperability. According to a narrower interpretation of the hindrance requirement, portability would not place an affirmative obligation on the original controller to transfer data directly, it would, rather, seek to prevent a data controller from technically impeding the transfer of data to another controller. The latter interpretation would indeed reduce costs for the original controller, however, the text and rationale of the right support a broad interpretation, as an obligation to provide seamless exportation tools is clearly placed upon the data controller. Industry stakeholders suggest that a solution for direct data transfers, in some instances, could be the "data-pull model". This model would enable individuals and the receiving provider to agree on appropriate processing of data before the transfer, it would not require competing services to understand the internals of other services' systems and would incentivize the receiving provider to create tools to absorb transferred data and gain potential new customers. See Centre for Information Policy Leadership, *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016,* 15 February 2017, 4.

[86] See European Commission, *Impact Assessment*, cit., 106. The assessment also notes that use of existing interfaces for these purposes would allow the development of portability functions very quickly.

[87] See e.g., A. Diker Vanberg, *The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?*, in *Journal of Internet Law*, 21(7), 2018, 13-14; P. Swire - Y. Lagos, *op. cit.*; R. H. Weber, *Data Portability and Big Data Analytics*, cit., 66-67; Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"*, cit., 2. The CIPL report suggests that an overly broad implementation of the right may entail unrealistic efforts for controllers

Conclusively, controller-to-controller data portability is an ambitious and innovative feature of Art. 20 GDPR. As users may typically be uninterested in a pure data export, the full enjoyment of the right and thus, the empowerment of data subjects, rely on the ability to effectively exercise this dimension of the right in practice and its enforceability against a non-compliant controller. Pressure from data subjects requesting direct and automatic portable transfers should compel data controllers to provide seamless technical feasibility and abide by Art. 20(2).

4.3 A broad balancing clause: Art. 20(4)

Art. 20(4) of GDPR states that the right to data portability «shall not adversely affect the rights and freedoms of others». This provision refers to the circumstance where a dataset includes data concerning multiple subjects other than the requesting data subject. Nonetheless, the Regulation is silent on the approaches to address and settle conflicts involving the rights and freedoms of third parties.

The clause is intended to avoid data retrieval and transmission of non-consenting data subjects to a new data controller, in cases where these data are likely to be processed in ways that would negatively impact their rights and freedoms, e.g., if the transfer prevents other data subjects from exercising their rights under the GDPR. The wording provides a broad and general balancing clause, yet, does not grant a prevalence of other rights over data portability, but merely, a "non-prevalence" rule between conflicting rights.[88]

Where personal data of other subjects are contained in a dataset, another legal basis for processing must be identified. In these circumstances, the data of third parties may be legitimately processed by the controller where it does so on the basis of a legitimate interest pursuant to Art. 6(1)(f) of GDPR.[89] Importantly, responsibility for potential impacts on third parties appears to rest on requesting data subjects, to the extent that the data controller does not determine the processing in any way.[90]

Generally, the rights of third parties will be respected where their transferred dataset is processed for the same purposes as those stated by the original transmitting controller. Therefore, the receiving data controller may not use third-party personal data for their

to set up workable technical systems. In many situations, providers will have to make substantial investments to create compatible ICT infrastructures and APIs. On the one hand, the exercise of the right should not be restricted, while on the other, disproportionate efforts on part of providers should not be imposed, particularly in those cases where portability does not award added value to individuals.

88 P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit*., 6. See also Article 29 Working Party, *Guidelines on the right to data portability*, cit., 11.

89 Article 29 Working Party, *Guidelines on the right to data portability,* cit., 11. Examples may be in the context of a webmail service or bank account, where contacts containing personal information of other individuals are included. It is unlikely here that the rights and freedoms of third parties are adversely affected, where the use of that information remains, under the new data controller, processed for the same purpose (e.g. to form history of the account or to be used as contact addresses).

90 *Ibid*. In other words, according to the WP29, if personal data relate to the data subject or to a third party, it is responsibility of the requesting data subject to ensure that data protection rights of third parties are respected. See also A. Diker Vanberg, *The Right to Data Portability in the GDPR,* cit., 12.

own purposes without knowledge and consent of the party involved.[91] The WP29 further recommends that data controllers implement tools enabling data subjects to select the relevant data they wish to have ported, and where relevant, exclude personal data regarding other subjects. Data controllers should, moreover, implement consent mechanisms to ease the transmission of data for those cases where third parties are willing to consent.[92] In practical terms, where the data controller may legitimately deny a portability request violating the rights of a third party, the delimitation will likely discourage data subjects from invoking their right to data portability.[93]

Art. 20(4) also covers the rights of data controllers. Although there is no explicit mention in Art. 20 nor in Recital 68, Recital 63 on the right of access maintains that «rights and freedoms of others» include «trade secrets or intellectual property and in particular the copyright protecting the software». The 29WP's Guidelines only incidentally address this issue, by maintaining that «the result of those considerations should not be a refusal to provide all information to the data subject», as provided in Recital 63 and moreover, that the controller should not reject a portability request based on the infringement of other contractual rights. Whereas it specifies that the individual may not misuse information obtained under Art. 20 in ways that may qualify as unfair practices or that violate intellectual property rights, it affirms, on the other hand, that potential business risks cannot in and of themselves serve as a basis for refusing portability, insofar as controllers transmit data in a form that does not disclose information covered by trade secrets or intellectual property rights.[94] While the recommendation is meant to

[91] Article 29 Working Party, *Guidelines on the right to data portability, cit.*, 12; P. Voigt - A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A practical Guide*, Dordrecht - Heidelberg - London - New York, 2017, 172-173. The WP29 recommends that social network providers should not enrich the member profiles by using personal data transmitted by data subjects through a portability request. They must respect the principle of transparency and ensure they rely on an appropriate legal basis for each processing operation. Neither can the third party data be used to retrieve information about them or create specific profiles, even if the provider already holds data regarding the third party.

[92] Undue limitations placed on the GDPR regime may interfere with the results originally pursued. See O. Lynskey, *Aligning data protection rights with competition law remedies? The GDPR right to data portability,* cit., 814. Guidance on this point is controversial and not sufficiently clear. The WP29's recommendations on this point may place an unreasonable burden on both transmitting and receiving controllers. In fact, the position contradicts the approach supporting a broad definition of data «concerning the data subject». See Article 29 Working Party, *Guidelines on the right to data portability*, cit., 9. This aspect will be further discussed *infra* in paragraph 4.4. Furthermore, the fact that the receiving controller must determine a legal basis for processing third party data seems unreasonable, given that such data is "incidental" and its legitimacy may be obvious in many cases. See Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability",* cit., 9. DigitalEurope, representing digital technology industry in the EU, encourages to include further considerations for the protection of third parties, i.e.: proportionality of the amount of requested data, purpose for which the right is exercised, feasibility or complexity of separating other subject's data, usability of the ported data when third subject's data are excluded and the actual legal basis on which the personal data of third parties can be transferred to another data controller without their consent. See DigitalEurope, *DigitalEurope's views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242)*, Brussels, 1 February 2017, 3-4.

[93] A. Diker Vanberg - M. B. Ünver, *The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*, cit., 3.

[94] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 12; P. Voigt - A. von dem Bussche, *op. cit.*, 173. Organizations should be able to strip valuable data from requested datasets if it adversely affects trade secrets and IP rights. See A. Diker Vanberg - M. B. Ünver, *The right to data portability in the*

prevent the depletion of the right and non-compliance, it must be ensured that it works in a balanced manner. Greater flexibility in recognizing competing rights and interests involved is worth consideration. This entails ensuring that legally protected rights be respected and impeding that organizations acquire unfair advantages.[95] In practice, it will be for the courts to establish on a case-by-case basis whether the exercise of data portability adversely impacts third-party rights in each specific circumstance.
In sum, it appears that the GDPR may have underestimated the number of conflicts involving third party rights and this provision, contingent upon the interpretation that will be adopted by the European Data Protection Board and settled by the courts, may significantly impair the reach of the right.

4.4 Types of data covered by data portability

According to Art. 20(1), personal data falling under its scope must, firstly, «concern» the data subject requesting portability and secondly, be «provided by» the data subject to a controller. Data that is not personally identifiable, such as anonymized data, are excluded from the GDPR regime, whilst pseudonymous data, which merely reduces the linkability of a dataset with the original identity of a subject, are bound to fall within the scope of Art. 20.[96] Typically, controllers will process datasets containing personal data of several data subjects. In this context, data controllers should not adopt too restrictive an interpretation of data «concerning the data subject» involved in processing operations. In these cases, the data subject issuing a portability request shall obtain access and receive those records. However, where those datasets are directly transmitted to a new data controller, the receiving controller shall not process the data for any purpose, which would adversely impact the rights and freedoms of the other data subjects and third parties whose information is included in those records.
The second condition required by Art. 20(1) is that personal data concerning a data subject must be «provided by» the data subject. This provision restricts the material scope of portable data.[97] Firstly, an individual actively and knowingly providing their

GDPR and EU competition law, cit., 5. While individual data will hardly qualify as a trade secret, pursuant to *Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, OJ L 157, 15.6.2016, the combination of data and information may well do so. See J. Drexl - R. M. Hilty - L. Desaunettes *et al.*, *Data Ownership and Access to Data*, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, Research Paper no. 16-10, 7. For an overview of the right's interplay with IP regimes, see I. Graef - M. Husovec - N. Purtova, *op. cit.*, 11-18.

[95] Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability",* cit., 10.

[96] The rule is derived *a contrario* from Art. 11(2) of GDPR. The provision states that, where processing does not require identification and the data controller is able to demonstrate that it is not in a position to identify the data subject, among other rights, portability shall not apply «except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification». Although this could cover pseudonymous data, the data controller is not under a positive obligation to acquire additional data to identify the data subject pursuant to Art. 11(1) and Recital 57 of GDPR.

[97] A strict interpretation of the definition «provided by the data subject» may lead to unrealistic results.

personal information to the data controller, e.g., when creating an online account, typically submitted through online forms and tools of a website or mobile application. Broadly speaking, the individual performs direct actions, aware of the fact that they result in the origination of data. Whereas the individual may be unaware of the linked implications, the fact that data is, nevertheless, being created should be «obvious – or at least intuitive».[98]

Secondly, online providers will often hold more varied troves of data, such as those obtained through observation of the activities related to the use of their service. In particular, this type of data, so-called "observed data", is observed and recorded in a digital format, either at the moment of their creation, or transmitted to a digital carrier after observation. While individuals may be aware that observed data is created (through active engagement, for instance), it may nonetheless go unnoticed for the better part. On this point, the Article 29 Working Party has clearly advised that the definition of data «provided by the data subject» be interpreted as including personal data observed from online user activities.[99] Including observed data resulting from on-

For instance, in the case of data ported within an email service, a restrictive interpretation would include in the scope of Art. 20 merely outgoing emails (actively provided by the data subject), whilst incoming emails (provided by other individuals) would not be subject to portability. See T. J. McIntyre, *Making sense of the right to data portability*, speech at *CDPC 2016 Invisibilities & Infrastructures 9th International Conference*, Brussels, 27-28-29 January 2016.

[98] Working Party on Security and Privacy in the Digital Economy, *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, Summary of the OECD Privacy Expert Roundtable, 21 March 2014, 5. This type of data may be categorized and distinguished based on the context in which data are originated, i.e.: data disclosed by individuals in the context of a loan application ("initiated data"), data created when buying a product with a credit card ("transactional data"), or data shared (actively) via an online social network ("posted data").

[99] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 9-10. The EDPS advised that the right be given a wide scope of application, not limited to the processing operations using data provided by the data subject. See European Data Protection Supervisor, *EDPS recommendations on the EU's options for data protection reform*, cit., 12 at fn. 34. However, a broad interpretation of the definition of "observed data" may lead to unjustified impacts on intellectual property rights and trade secrets. Online services and platforms may restrict the download or transfer of data covered by intellectual property or other restrictions, as is, e.g., the case of Facebook's "Terms of Services on Safety". See Centre for Information Policy Leadership, *GDPR Implementation Challenges: A Summary of CIPL GDPR Project Participants' Feedback,* 27 April 2017, 7. See also Working Party on Security and Privacy in the Digital Economy, *Protecting Privacy in a Data-driven Economy*, cit., 5. Examples of observed data may be e.g. search histories, activity logs, traffic data, location data, as well as raw data processed by smart meters and smart objects, data originating from online cookies, generated by sensors, and passively created observational data (e.g. captured by CCTV cameras combined with facial recognition). However, the Centre for Information Policy Leadership supports a stricter interpretation. Comparing the wording of Art. 20 with Art. 13 on access, a discrepancy emerges, where the former refers to data «provided by» the data subject and the latter to data «collected from» him or her. This raises the question whether "observed" data falls under the scope of "provided" data, as held by the WP29, or if it is more likely to qualify under a passive dimension, i.e. "collection from" the data subject. Given that individuals often do not have an active role in the creation process of observed data, it may seem correct to treat those data as being merely collected and thus, beyond the scope of application of Art. 20, facially referring to active provision. Observed data may fall within or out of the scope of portability depending on whether the data is inextricably linked to the service in question and thus, provided by the individual (e.g. wearable tracking devices collect raw data for the specific purposes of the service, which awards added value and of which the individual is typically aware of), or when the data essentially constitutes a byproduct of technical analysis (e.g. network traffic data), generated by systems and not provided by the individual in return for a particular benefit or as part of the service. See Centre for Information Policy Leadership, *Comments*

line activities may allow data subjects to gain a better understanding of implementation choices of the data controller.

Moreover, it should allow individuals to broadly appreciate the extent to which their fundamental right to informational privacy is respected.[100] The objectives underlying the data protection reform generally, and the right to data portability specifically, support a broad interpretation of the term «provided by the data subject» for the purposes of effective protection and guaranteeing that data subject rights are not impaired by arbitrary choices of service providers.

Thirdly, data may also be created on the basis of provided data, yet be autonomous. Those are "derived" and "inferred" data, respectively, generated by other data or constituting a product of probability-based analytical processes.[101] Whether data are derived from the analysis of actively provided data, or constitute the outcome of an assessment regarding a data subject or their profile, they cannot be considered as «provided by» the data subject for the purposes of Art. 20(1) and thus, fall outside its scope of application. Indeed, secondary data not only goes beyond the text of Art. 20, but may also hinder other rights, for instance, those protected by trade secrets, intellectual property and other legally protected interests. Nonetheless, the data subject may still exercise relevant rights covering inferred or derived data regarding him or her, in particular, through the right of access. As demonstrated, the types of data that may be ported are limited to certain restricted categories of data.[102]

Part of scholarship devised two opposite practical options based on the interpretation of Art. 20 of GDPR. Firstly, a minimum approach encompasses merely data that are

on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability", cit., 8. Moreover, other industry stakeholders hold that including observed data in the definition places a disproportionate obligation on telecom operators and is not practical. See European Telecommunications Networks Operators' Association, *Legal memo with respect to the Article 29 Guidelines on the right to data portability*, 170131 ETNO Data Portability Memo, 16 February 2017, 8-9; DigitalEurope, *DigitalEurope's views on Article 29 Working Party draft Guidelines on the right to data portability*, cit., 5.

[100] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 9-10.

[101] "Derived data" constitute new data elements related to a specific individual. Data belonging to this category are created in a fairly mechanical manner, by way of simple reasoning and basic mathematics, which detect patterns within a dataset and create subsequent classifications. Although classifications as such may well be used for predictive purposes at a later stage, they are not in themselves based on probabilistic reasoning. Examples of derived data are: computational data (e.g. calculation of customer profitability based on the ratio between number of visits and items bought) and notational data (e.g. detection of common attributes among "profitable" customers used to classify potential customers). "Inferred data" constitute the outcome of detecting correlations, in turn, used to create predictions about behaviors, then used to categorize individuals. Examples of inferred data are statistical data (e.g. credit risk scores, life expectancy scores) and advanced analytical data (e.g. likelihood of future health outcomes based on an analysis of large and diverse medical datasets). These types of data may also be created in contexts that are different and unrelated to the purposes of the original data collection or of the processing. Typically, the data subjects to whom the inferred data pertains are not aware of inferences made about them, nor are they involved in its creation. See Working Party on Security and Privacy in the Digital Economy, *Protecting Privacy in a Data-driven Economy*, cit., 5.

[102] Data controllers must take into consideration that individuals are typically unable to evaluate what data is relevant for portability purposes. A useful option may be to rely on standard download functionalities in the provider's systems, in order to create CSV or other types of files with no systematic ability to tailor the dataset. See Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"*, cit., 3-4.

explicitly provided to the data controller. In this case, the right is inherently linked to the right's dimension of data withdrawal from the original data controller (the "*adieu* scenario"). Secondly, an extensive approach, relying on a wide interpretation of data «provided», including observed data, in combination with controller-to-controller data portability, allows a "fusing scenario" promoting the interconnection of services.[103]
Whilst the second scenario positively drives towards the creation of user-centric platforms, in the writer's opinion, interpretations should be nuanced, considering whether data portability provides individuals with added value in a specific circumstance. Therefore, in contexts where general-purpose data portability does not award any meaningful value, Art. 20 could be subject to a narrower interpretation and avoid overburdening data controllers.

4.5 Making data portability meaningful: interoperability and standardization of data formats

Recital 68 of the GPDR encourages data controllers to develop interoperable formats enabling data portability, but at the same time, it weakens its reach by explicitly stating that the provision does not create an obligation for providers to adopt, nor maintain, technically compatible processing systems.[104] Whereas EU legislative instruments provide an array of different definitions of interoperability in different contexts, a well-fitting definition is semantic interoperability, i.e. the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results, as defined by end-users. This entails that the "meaning" of the data is transmitted and is, in turn, necessary to allow re-usability of those data. Technical compatibility, on the other hand, is only incidentally mentioned as part of the definition of data integration, that is, the combination of data from different sources.[105]
Based on the wording of Recital 68, data portability aims to produce interoperable systems, not compatible ones. Although the distinction is not clear-cut, given the wide range of types of data that may be processed by online providers, the Regulation does not impose specific recommendations on what data format must be provided. On this point, the Article 29 Working Party specifies that appropriate data formats will vary, they must, however, be chosen in light of the purpose of being interpretable, in order to allow re-usability, hence, allowing the data subject to exercise his or her rights.[106]

[103] P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 11.

[104] Nonetheless, the implementation of specific software seems necessary, as it is unclear how the right could be exercised if the two communicating systems do not embed a compatible export-import module. See L. Scudiero, *op. cit.*, 120. As to the understanding of the terms, it is not clear what the exact difference, if any, exists between interoperability and technical compatibility. Broadly speaking, interoperability, within the context of ICTs, is the ability to transfer and make data and information useful across systems, applications or components. See J. Palfrey - U. Gasser, *Interop, The Promise and Perils of Highly Interconnected Systems*, New York, 2012, 5-8. On the other hand, different datasets are compatible where they «use the same names for the same objects, the same units or coordinates, etc.» See EU Glossary.

[105] EU Glossary, cit.

[106] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 17. Along these lines, data

Indeed, data portability may well remain an unworkable tool for individuals where personal data formats are not standardized.[107] Therefore, Art. 20(1) seems a call for interoperability and standardization directed at industry stakeholders. Art. 18(3) of the Draft Regulation endowed the European Commission with the power to specify the electronic format, technical rules, modalities and procedures for data transmission with particular regard to the implementation of the right to data portability. The removal of this provision from the final text of the Regulation is justified on grounds of technological neutrality and has eliminated the initially envisaged "standardization role" of the Commission.[108] Nonetheless, the issuance of recommendations on the specification of formats and technical aspects would be advisable, likely a task to be addressed by the newly established European Data Protection Board.[109] What is recommended by the 29WP is that the data formats used should have a high level of abstraction from any internal or proprietary format. In this sense, data portability entails an additional layer of data processing by controllers, in order to extract personal information from the platform and filter out data which do not fall in the scope of the right, such as, for instance, inferred data or those related to security.[110] Without interoperable formats and standards, which allow for an easy and seamless data sharing, as well as a cost-effective implementation, the right's effectiveness would essentially be depleted.[111] It would frustrate the right's "controller-to-controller" dimension, as direct data transmission would prove unworkable in practice, likewise, the data retrieval right of individuals, who must be able to read, understand and re-use the dataset with little or no effort. Therefore, an effective right to data portability is consequential to attain-

formats that are subject to costly licensing constraints are not considered adequate.

[107] Be noted, an initiative for data standardization is on foot, see European Commission, *ICT Standardisation Priorities for the Digital Single Market*, COM(2016) 176 final, 9, 2016. The initiative does not specifically cover the right to data portability, but as it will likely impact the major domains of cloud computing and the Internet of Things, the Commission has set both as standardization priorities. Cloud computing services in particular, will, in turn, be a crucial sector for data subjects to exercise the right to data portability.

[108] Council of the European Union, Interinstitutional File: 2012/0011 (COD), 5879/14, 31 January 2014, 3. See also P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 4; P. Voigt - A. von dem Bussche, *op. cit.*, 174.

[109] See Art. 68 of GDPR. The removal of the provision from the Draft Regulation could be due to a fear of a pervasive interference of the European lawmaker in technology areas, typically left to self-correction by market forces. See *Note from the Presidency of the Council of the European Union to the Working Group on Information Exchange and Data Protection (DAPIX)*, 47. Authors have remarked that collaboration among market players is crucial in devising industry norms and standards to this end. See A. Diker Vanberg - M. B. Ünver, *op. cit.*, 4. Within the context of interoperability and data portability relating to cloud services, the creation of standards that are voluntary, industry-led, global and open is advised. See European Parliament, *Cloud computing, an overview of economic and policy issues*, European Parliamentary Research Service, 26 May 2016, 20; DigitalEurope*, DigitalEurope's response to the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, 18 December 2015. The approach was also confirmed in the context of Internet of Things solutions. See European Commission, *Rolling Plan for ICT Standardisation - 2017*, Executive Summary, COM(2016) 176 final, n. 11, 24.

[110] Article 29 Working Party, *Guidelines on the right to data portability*, cit., 17.

[111] European Data Protection Supervisor, *Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, cit., 13; I. Graef - M. Husovec - N. Purtova, *op. cit.*, 19-20.

ing a certain degree of interoperability of information systems used by digital service providers.[112]
As the sections *supra* have demonstrated, months after the entry into force of the GDPR, interpretative and technical uncertainties remain open and are likely be settled by the courts, if and when litigation on data portability arises.

5. Concluding remarks

Scholarship has proposed a systematic interpretation of Art. 20, supporting a pragmatic and extensive approach, in order to benefit from the interrelationship that this regulatory tool can have with regards to the Digital Single Market and the fundamental rights of individuals in the online world.[113] Nonetheless, given that many implementation issues remain unresolved, it would be reasonable to balance the provision's effects with the burdens placed on data controllers, insofar as the right does not produce added value for users in specific circumstances.
This article presented the ambitious objectives set out by the GDPR for the purposes of attaining transparent data control. If properly implemented, the right to data portability presents a valuable opportunity to develop a user-centric interconnected digital environment. Nevertheless, this articles casts doubt upon the significance of the provision's reach. The primary objective of the general right is for individuals to reclaim control over their personal data and thus, attempts to rebalance power asymmetries in the online world. In practice, the beneficial impacts of the right and the achievement of a greater degree of user control largely depend on the extent to which individuals will exercise the right in practice and will hold data controllers accountable for complying with their obligations under the data protection framework.
Furthermore, this article has demonstrated that the right to data portability applies in a reduced range of situations and that several conditions may severely limit its practical functioning. In its basic dimension, Art. 20 vests data subjects with the right to obtain their personal datasets in formats that support re-usability. The innovative "controller-to-controller" portability feature, pursuant to Art. 20(2), can only be properly achieved where technically compatible and interoperable solutions are in place to ensure swift and seamless direct data transfers. Moreover, Art. 20(4), providing a broad balancing clause, raises concerns for third-party data that will be contained in a majority of datasets. In fact, the EU regulator may have underestimated the number and extent of potential conflicts and the clause, ultimately, is capable of appreciably limiting the incidence of the right.
The proven limited exercisability of the general right to data portability puts into question the intensity of the alleged control granted to data subjects and its ability to enhance the informational self-determination of European online users. Contrary to its objectives, the GDPR may have adopted too optimistic a view, as data portability may

[112] S. Sica - V. D'Antonio - G. M. Riccio, *op. cit.*, 238.

[113] P. De Hert - V. Papakonstantinou - G. Malgieri - L. Beslay - I. Sanchez, *op. cit.*, 11. For an argument in favor of a minimalistic and conservative approach, see P. Przemysław Polański, *op. cit.*, 146.

even clash with the right to data security. A decreased level of security would produce more harmful effects on individual privacy rights than the potential benefits of portability and instead of empowering data subjects, it could rather increase risks of data breaches in cyberspace and cause an even greater loss of individual control.