Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The right to data portability in the GDPR: Towards user-centric interoperability of digital services

Paul De Hert [a,b], *Vagelis Papakonstantinou* [a], *Gianclaudio Malgieri* [a], *Laurent Beslay* [c], *Ignacio Sanchez* [c,*]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *Tilburg University (TILT), The Netherlands*
[c] *European Commission, Joint Research Centre (JRC), Italy*

Keywords:
EU data protection
EU General Data Protection Regulation
Right to data portability

A B S T R A C T

The right to data portability is one of the most important novelties within the EU General Data Protection Regulation, both in terms of warranting control rights to data subjects and in terms of being found at the intersection between data protection and other fields of law (competition law, intellectual property, consumer protection, etc.). It constitutes, thus, a valuable case of development and diffusion of effective user-centric privacy enhancing technologies and a first tool to allow individuals to enjoy the immaterial wealth of their personal data in the data economy. Indeed, a free portability of personal data from one controller to another can be a strong tool for data subjects in order to foster competition of digital services and interoperability of platforms and in order to enhance controllership of individuals on their own data. However, the adopted formulation of the right to data portability in the GDPR could benefit from further clarification: several interpretations are possible, particularly with regard to the object of the right and its interrelation with other rights, potentially leading to additional challenges within its technical implementation. The aim of this article is to propose a first systematic interpretation of this new right, by suggesting a pragmatic and extensive approach, particularly taking advantage as much as possible of the interrelationship that this new legal provision can have with regard to the Digital Single Market and the fundamental rights of digital users. In sum, the right to data portability can be approximated under two different perspectives: the minimalist approach (the adieu scenario) and the empowering approach (the fusing scenario), which the authors consider highly preferable.

* *Corresponding author.* European Commission, Joint Research Centre (JRC), Directorate for Space, Security and Migration, Cyber and Digital Citizens' Security, Via E. Fermi 2749, I-21027 Ispra (VA), Italy.
E-mail address: ignacio.sanchez@ec.europa.eu (I. Sanchez).

https://doi.org/10.1016/j.clsr.2017.10.003

1. Introduction

The right to data portability is one of the most important novelties within the EU General Data Protection Regulation[1] (hereafter: GDPR), both in terms of warranting control rights to data subjects and in terms of being found at the intersection between data protection and other fields of law (competition law, intellectual property, consumer protection, etc.).

The first example of portability of users' data referred to telephone numbers. In the GDPR text it was extended to all digital services. It constitutes, thus, a valuable case of development and diffusion of effective user-centric privacy enhancing technologies and a first tool to allow individuals to enjoy the immaterial wealth of their personal data in the data economy. Indeed, a free portability of personal data from one controller to another can be a strong tool for data subjects in order to foster competition of digital services and interoperability of platforms and in order to enhance controllership of individuals on their own data.[2] However, the adopted formulation of the right to data portability in the GDPR could benefit from further clarification: several interpretations are possible, particularly with regard to the object of the right and its interrelation with other rights, potentially leading to additional challenges within its technical implementation.

The aim of this article is to propose a first systematic interpretation of this new right, by suggesting a pragmatic and extensive approach, particularly taking advantage as much as possible of the interrelationship that this new legal provision can have with regard to the Digital Single Market and the fundamental rights of digital users.

In this context, Section 2 will outline the legal and historical background of the right to data portability: examples of information portability before the GDPR approval will be given, and the way it was provided for in the first European Commission Proposal for the GDPR will be elaborated. Section 3 will discuss the rationale and impact of data portability, particularly with reference to it constituting a step towards data ownership while also being a problematic right in terms of interests and freedoms of others. Section 4 includes the textual analysis of Article 20 of the GDPR: three different rights broadly fall under the "data portability right" and several balancing clauses need to be analysed in this regard. In particular, one concrete issue is the interpretation of the *object* of data portability: Section 5 addresses two different approaches (extensive and restrictive) to the interpretation of which personal data can be ported, with respective arguments and counterarguments. These two different approaches affect also the relationship of portability with other rights (particularly the right to access and the right to erasure), this is why Section 6 will explore this issue. In sum, the right to data portability can be approximated under two different perspectives: the minimalist approach (the *adieu* scenario) and the empowering approach (the *fusing* scenario), which we consider highly preferable, as outlined in Section 7.

2. Background and rationale

The right to data portability is a full novelty in the EU data protection framework, since in the Data Protection Directive (95/46/EC) text no relevant references may be found. In fact, no field of law has experimented before with anything resembling to personal data portability.[3] Actually, in the EU legal framework there are some small references to portability, particularly in the telecommunication sector, e.g., the "Universal Service Directive" (2002/22/EC)[4] at Article 30 (as well as recitals 40–42) refers to "number portability".[5] The portability of telephone numbers is the theoretical and practical precursor of data portability.[6] A further step towards portability of information (not only of numbers) can be found in the "Framework Directive" (2002/21/EC)[7] at recital 31, where interoperability of Application Program Interfaces

[1] 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) (Text with EEA relevance).

[2] See Article 29 WP, *Guidelines on the right to data portability*, 16/EN, WP 2042, rev01, as last revised and adopted on 5 April 2017, p.6. See also, European Commission, Building a New Data Economy Communication (January 2017), https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[3] B. CUSTERS, H. URSIC, Big Data and Data Reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection, International Data Privacy Law, 7 January 2016, 9. However, see interestingly the new French Law (Loi n. 2016-1321 du 7 Octobre 2016 pour une République numérique) which, though approved after the approval of GDPR, is the first example of national law implementing the right to data portability. It has been introduced in the Code de la Consommation (Article 48, with reference to GDPR), as a right which only applies in the consumer area. See also the proposal to provide a portability of bank account number across the EU, see in particular Expert Group on Customer Mobility in Relation to Bank Accounts, Report, 5 June 2007, Brussels, http://ec.europa.eu/internal_market/finservices-retail/docs/baeg/report_en.pdf (accessed 25 May 2017).

[4] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[5] See also European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (Preliminary Opinion) (March 2014), 15, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf (accessed 27 February 2016).

[6] See I. GRAEF, Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union (22 July 2013). Telecommunications Policy 2015, Vol. 39, No. 6, p. 502–514.

[7] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

systems is considered useful for the portability of interactive contents.[8]

Article 29 Working Party (hereafter: WP29), in its recent guidelines on the right to data portability, highlights potential "synergies and even benefits to individuals" between these types of portability and the new personal data portability "if they are provided in a combined approach, even though analogies should be treated cautiously".[9]

Within the specific field of personal data protection, the portability of personal information has been encouraged even before the approval of GDPR. Interestingly, WP29, in its opinion on purpose limitation[10] states that allowing "data portability could enable businesses and data-subjects/consumers to maximise the benefits of big data in a more balanced and transparent way. It can also help minimise unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes, which would benefit both businesses and data-subjects/consumers". What arises from this reflection is that the right to data portability is considered in its widest scope (portability of any data useful for decision-making purposes). We will see *infra,* that the adopted version of the right to data portability in GDPR can benefit from further explanations on this point.

Regarding the notion of legitimate interest in the WP29 opinion, data portability is considered as an "additional safeguard" applied by data controllers, which may "empower data subjects" and it therefore constitutes a positive element in the balancing test between data controllers' legitimate interests and data protection rights of subjects. In the words of WP29, data portability should be part of the general "availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data".[11] Interestingly, the reflections of WP29 are very similar to the formulation of the final version of the right to data portability.

Indeed, the first attempt to regulate the right to data portability was noted at Article 18 of the European Commission Proposal for the General Data Protection Regulation:

> *"1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.*
>
> *2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.*
>
> *3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."*

Consequently, in that version the idea of data portability was first introduced, taking into consideration digital platforms, and also in order to deal with the alleged lock-ins of internet social networks.[12]

At the same time, in its first comment on this new proposed idea of data portability, WP29 highlighted that this should not only be a "data protection right", but a more *economic* right: "in many situations, safeguards such as allowing data-subjects/customers to have direct access to their data in a portable, user-friendly and machine-readable format may help empower them, and *redress the economic imbalance between large corporations on the one hand and data-subjects/consumers on the other*. It would also let individuals *'share the wealth'* created by big data and incentivise developers to offer additional features and applications to their users".[13]

In sum, WP29 highlights the great potentialities of a full portability of personal data: "empower[ing] data subjects and let[ting] them benefit more from digital services. *In addition,* it can foster a more competitive market environment, by allowing customers more easily to switch providers *(e.g., in the context of online banking or in case of energy suppliers in a smart grid environment). Finally, it can also contribute to the* development of additional value-added services by third parties who may be able to access the customers' data at the request and based on the consent of the customers. *In this perspective, data portability is therefore not only good for data*

[8] "Open APIs facilitate interoperability, i.e., the portability of interactive content between delivery mechanisms, and full functionality of this content on enhanced digital television equipment. However, the need not to hinder the functioning of the receiving equipment and to protect it from malicious attacks, for example from viruses, should be taken into account". See Also, Article 29 WP, *Guidelines on the right to data portability,* supra, p. 15 where APIs are encouraged in order to deal with the request of portability right in case of a large or complex personal data collection.

[9] Article 29 WP, *Guidelines on the right to data portability, supra*, p. 4.

[10] Article 29 WP, Opinion 03/2013 on purpose limitation, WP 203, p. 47.

[11] *Ibidem*, p. 46–47.

[12] See recital 53 of the European Commission for the GDPR ("The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one"). This reference has been then removed in the final part. B. CUSTERS, H. URSIC, *Big Data and Data Reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection*, International Data Privacy Law, 7 January 2016, 8; I. GRAEF, J. VERSCHAKELEN and P. VALCKE, *Putting the Right to Data Portability into a Competition Law Perspective* (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53–63. See also G. Zanfir, The Right to Data Portability in the Context of the EU Data Protection Reform, 11 May 2012, IDPL 11.

[13] Opinion 06/2014 on the notion of legitimate interests of the data controller under 95/46/EC Directive. See also B. CUSTERS and H. URSIC, supra, about the role of data portability in "reusing" the wealth of personal data.

protection, but also for competition and consumer protection"[14] *(italics added)*.

Moreover, the European Data Protection Supervisor in his 2015 recommendations on the EU data protection reform[15] has considered data portability to be a strategic element. In particular, portability of personal information was seen as the "gateway in the digital environment to the user control which individuals are now realising they lack". Thus, he recommended that, in order to be effective, the right to data portability must have a wide scope of application, and not only be applied to the processing operations that use data provided by the data subject.

3. Textual analysis of Article 20, GDPR: three rights in one and wide balancing clauses

The new version of Article 20, GDPR sets that:

> "1. *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*
>
> *(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and*
>
> *(b) the processing is carried out by automated means.*
>
> 2. *In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.*
>
> 3. *The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*
>
> 4. *The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.*"

A first observation refers to the fact that there are several points of difference between the original Commission proposal and the finally adopted GDPR text: the *object* and the *exercise* of the right, the *format* of data, the *Commission* role, the *balancing* clauses, and the *relationship with the right to be forgotten*. In more specific terms, the *object* of portability is now more limited and precise. While the first proposal referred to "a copy of data undergoing processing", the final version refers to "personal data *concerning him or her*, which he or she *has provided to a controller*". Therefore, in the final approved version, only data concerning specifically the data subject can be "ported" and only if he/she has provided them.[16]

The *exercise* of the right to data portability has also been further developed in the final text of the GDPR. In the original, Commission, version, the right consisted in obtaining a copy of data and, at certain conditions, transmitting it to another data controller. Instead, in the final version it has been reformulated so as to also allow individuals to "have the personal data *transmitted directly* from one controller to another, where technically feasible".[17]

The *format* of data is a crucial element. In the original Commission proposal, it was an "electronic", "structured" and "commonly used" format that "allows for further uses", while the approved version refers only to "machine-readable" format. We can thus observe that the format standard has been reduced to a minimum (machine-readable).[18]

The Commission's role in the first proposal is a crucial role towards data portability implementation and towards an effective interoperability of services (Article 18(3)). Indeed, the European Commission's role was conceived as a progressive specification of data format, but also for "technical standards, modalities and procedures for the transmission of personal data". In other words, it could have helped to conform normative standards to technological developments and it could have fostered a concrete and effective development of interoperability of all digital services. Unfortunately, in the final version, such reference to the "standardisation" role of the European Commission has been removed.[19]

Another element of difference is the balancing with other interests. In the final version, there are several *balancing clauses*, which were not present in the initial proposal: the exercise of the right to data portability shall be "without prejudice" to the right to be forgotten (Article 20(3)) and "shall not adversely affect the rights and freedoms of others" (Article 20(4)). This new wording highlights a more prudent approach of the European legislator towards possible risks and conflicts with other rights of interests.[20]

In the final version, there is no more reference to the *withdrawal of data* from the first controller (Article 18(2), Commission proposal "from whom the personal data are *withdrawn*" vs. Article 20(1), final version "from the controller to which the personal data have been provided").[21]

In general, the final version is more prudent than the initial Commission proposal (a more restricted object, more specific balancing clauses, and fewer steps towards a real interoperability of services). At the same time, the final GDPR version is more oriented towards an interconnection of all digital services. This is evident in particular from the new right to "have

[14] See also on this point the European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the document communication building a European data economy{COM (2017) 9 final}, p. 47 addressing "data portability from an economic perspective".

[15] EDPS recommendations on the EU's options for data protection reform, (2015/C 301/01).

[16] See § 5, infra.

[17] See § 4, infra.

[18] See next §.

[19] See next §.

[20] See § 4, infra.

[21] See § 6 and 7 about the interaction between "portability" and "withdrawal".

data transmitted directly from one controller to another" and to the removal of any reference to the "withdrawal of data" from the first data controller. As we will argue *infra*, this may incentivise the development of user-centric platforms[22] where all digital services shall be more interconnected and so interoperable.

In sum, it becomes very clear that the right to data portability – in the final version of the GDPR – is composed of three different rights:

1) the right to receive (without hindrance from the data controller) data concerning data subject which he/she has provided (§1);
2) the right to transmit (without hindrance from the data controller) those data to another controller (§1); and
3) the right to have the personal data transmitted directly from one controller to another (§2).

While rights 1) and 2) can be exercised in any case where the processing is based on consent or on a contract and when the processing is carried out by automated means, right 3) needs one more condition: "where technically feasible". The format in which data should be transferred is "structured, commonly used and machine-readable",[23] but the reference to "technical feasibility" is not related to the structured and machine-readable format, but to the "interoperability" of systems, as outlined in recital 68 of GDPR.[24]

WP29 argues that the three format requirements at Article 20(1) are supposed to facilitate the interoperability of the data format provided by the data controller. In other words, "interoperability" is the expected result, while *structure, common use and machine-readability* are the indicated means.[25] Actually, as we will see *infra*, interoperability (especially in the final version of Article 20) is not mandatory but just "suggested", while the three "means"/requirements are mandatory by law (see Article 20(1)).

The meaning of *machine-readable* can be easily inferred from the field of the public sector information. In particular, recital 21 of Directive 2013/37/EU defines it as "a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it".[26] WP29 in its first "guidelines on data portability" explained that, for example, a .pdf document is not machine-readable, while a document with as many *metadata* as possible at the best level of granularity, since "preserv[ing] the precise meaning of exchanged information", should be considered machine-readable.[27] This ambitious goal[28] has been actually reduced in the revised version of WP29 guidelines,[29] where it requires "commonly used open formats (e.g., XML, JSON, CSV, etc.) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction". As such, "suitable metadata should be used in order to accurately describe the meaning of exchanged information".

As regards *interoperability* of systems, the European Commission has defined it as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems".[30]

Interoperability does not mean "compatibility", as recital 68 clarifies.[31] At the same time, WP29 in its recent guidelines highlights that the determination of the interoperable formats is sector-specific.[32]

A specific remark should be dedicated to third data subjects' rights. Indeed, the exercise of right to data portability may

[22] See Article 29 WP, *Guidelines on the right to data portability*, as firstly adopted on 13 December 2016, p. 5: "this right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject's control". In the revised version v01 this sentence has been removed.

[23] See supra, § 3.

[24] See supra, § 3.

[25] Article 29 WP, *Guidelines*, rev01, supra, 17.

[26] It also adds: "documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format".

[27] See also Article 29 WP, *Guidelines*, supra, as firstly adopted on 13 December 2016 p. 14.

[28] That can be defined "semantic interoperability". While the mere "syntactic interoperability" can be defined as "the ability of two or more computer systems to exchange information," semantic interoperability would be the "ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems". https://en.wikipedia.org/wiki/Interoperability (accessed 25 May 2017).

[29] Article 29 WP, *Guidelines*, rev01, supra.

[30] See European Commission, Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services' 1.2.2 which recalls the definition of interoperability provided by the European Interoperability Framework. See also the definition of ISO/IEC 2382-01: "the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have a little or no knowledge of the unique characteristics of those units". It is interesting also the functional definition of portability proposed by C. SAAD, '*The data portability landscape – An update*' (The Data Portability Project, 18 December 2008) http://blog.dataportability.org/2008/12/18/the-data-portability-landscape-an-update/ (accessed 25 May 2017): "Interoperability means that irrespective of who is providing or receiving the data, it should be provided in such a way that is agreed upon by the community so that the implementation is consistent irrespective of parties participating in the transaction".

[31] Recital 68, GDPR: "the data subject's right to transmit or receive personal data concerning him or her should not create an obligation from the controller to adopt or maintain processing systems which are technically compatible". See, however, Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*, 15 February 2017, p. 13 which highlights that "the distinction between 'interoperable' and 'compatible' is not in all circumstances sufficiently clear".

[32] Article 29 WP, *Guidelines*, rev01, supra, p. 17: "The most appropriate format will differ across sectors and adequate formats may already exist, but should always be chosen to achieve the purpose of being interpretable".

imply that also information from a third data subject are ported, e.g., because they are inseparable from the first data subject who is exercising the right. Actually, Article 20 states clearly that only "data concerning him or her" could be ported. This means that, unless there is consent from third interested parties, the object of data portability should be reduced only to data concerning exclusively the data subject. In terms of technical and organizational measures, this provision should encourage data controllers to collect and process personal data of each data subject separately and not in an aggregate format (as long as possible). Actually, the Article 29 Working Party, in its recent guidelines recommends taking not an overly restrictive interpretation of this provision, e.g., for what regards telephone records, etc.,[33] as soon as it does not "adversely affect the rights and freedoms of others" (Article 20(4), *infra*).[34]

A final remark should be dedicated to the balancing provisions of Article 20(3). It may happen that data controllers, in order to comply with users' requests of data portability, could adopt specific technologies (data trackers, personal data identifiers, etc.) in processing operations that could appear as unfeasible for a full erasure of personal data. Another risk might be that, in order to guarantee a full exercise of the right to data portability to all users, data subjects whose data are inseparable from other subjects' data could be prevented from having their data erased. In all these cases, Article 20(3) states a prevalence of right to erasure on the right to data portability.

Paragraph 3 also clarifies that data portability "shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". In other words, if data are processed for public interest purposes,[35] data subjects cannot ask to obtain that information, to transfer it or to have it transferred to another controller. This is the case, for example, of data processing for law enforcement purposes (e.g., crime detection, intelligence investigation) or for administrative purposes.

The rationale of this provision refers to the specific role held by the controller in this case: he is an official authority. Indeed, the need to empower control rights of individuals is generally perceived in the private sector, where a competition among peer (private) data controllers is well expected. The exercise of data portability in the public sector (i.e., when data processing is necessary for a public interest task) is beyond the rationale of the right to data portability.

Finally, paragraph 4 of Article 20 adds that the right referred to in paragraph 1 *shall not adversely affect the rights and freedoms of others*. This wording includes a very wide and general balancing clause ("rights and freedoms of others"). However, it does not grant full prevalence of other rights on data portability, but only a "non-prevalence" rule between conflicting rights.

It is irrelevant whether data portability affects other rights or freedoms; what is essential in this case is that this effect is not "adverse", e.g., it shall not create an unjustified damage or an illegitimate limitation to other rights or freedoms. In practice this means that judges will need to determine – on a case-by-case approach – when the right to data portability will *adversely* affect rights and freedom of others in a specific circumstance. A relevant contribution may be found in the balancing test elaborated by WP29 in its opinion on the notion of legitimate interest:[36] in case of a conflict between data subjects' rights (here: the exercise of data portability) and rights and freedoms of others (e.g., economic or proprietary interests of the data controller, right to data protection of third people, etc.) it may be necessary to take into account other elements as well (how data are used, reasonable expectations about data usage, relationship between controller and subjects, additional safeguards applied by the controller, etc.).

In sum, analysing the different wording of these balancing clauses, we observe three different degrees of "prevalence" of other rights on data portability. There is a minimum level of prevalence of the right to be forgotten on data portability (the exercise of data portability *shall be without prejudice*), an intermediate level of prevalence of "rights and freedoms of others" (*not adversely affecting*) and a full prevalence of public interests (*portability shall not apply*) on data portability.

We observe that this balancing structure is quite different from other balancing solutions adopted in the GDPR. In particular, Article 17 (right to be forgotten) provides a more detailed list of full-prevalence clauses: Article 17(3) enlists five specific cases in which right to erasure does not apply (right of expression; tasks carried out in the public interests or in the exercise of official authority; public interests in the area of health; scientific or historical research purposes or statistical purposes; and the establishment, exercise or defence of legal claims), while there are no references to the milder balancing clauses that we find in Article 20 ("without prejudice" and "not adversely affecting").

The reason of this difference is probably due to a more prudent approach of the EU legislator in regulating right to data portability than right to erasure. Since data portability is more subject to technological development and its impact on other subjects is still mostly uncertain, the choice of a wide balancing clause (not adversely affecting rights and freedoms of others) allows judges to adjust solutions on a case-by-case basis, considering future technological or practical challenges.

[33] Article 29 WP, *Guidelines*, rev01, supra, p. 9, which clarifies, however: "where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third parties".

[34] In particular, where personal data of third parties are included in the dataset, another ground for lawfulness of processing must be identified, e.g., "a legitimate interest under Article 6(1)(f) may be pursued by the data controller to whom the data is transmitted, in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity", Article 29 WP, *Guidelines*, rev01, supra, p. 11.

[35] Article 6(1)(e).

[36] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. See also L. MOEREL and C. PRINS, *Privacy for the homo digitalis, Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things*, Wolters Kluwer, 2016, 11.

4. The issue of "data provided" from the data subject to the controller

A number of critical points need to be raised with regard to the right to data portability, as included in the final version of the GDPR. First, the object of the right has been seen as particularly vague.[37] Article 20 refers to "*data* concerning him or her, *which he or she has provided* to a controller". As mentioned above, in the original Commission proposal the right to data portability referred to any "data undergoing processing". In the final approved version this has been amended as "personal data concerning him or her which he or she has provided to the data controller".

In principle, the restriction to data that are only "provided" may be a safeguard to the intellectual property of data controllers, particularly avoiding that the intellectual work of a digital service provider (data inferred about consumers, using complex algorithms) could be lawfully disclosed to competitive businesses for free.[38]

"Data provided" can be interpreted in two different ways: restrictively and extensively. According to the restrictive interpretation, "data provided" means only personal data that the subject has *explicitly provided* in a written or anyway explicit form, e.g., filling a registration form, answering to questions, etc. On the other hand, according to the extensive interpretation, "data provided" means all personal data that data controllers have collected upon consent or according to a contract, e.g., through GPS (location data), cookies, preferences, etc.

In particular, considering that companies in the new digital economy can obtain data of individuals in different ways, it has been argued that personal data – on the basis of their "source of production" – can be *received, observed, inferred* or *predicted*[39] by companies. While *inferred* or *predicted* personal data are "produced" by companies (e.g., through data mining), *received* and *observed* data are obtained directly from the data subject. In more specific words, personal data that data controllers "receive" from data subjects, are actively (and often spontaneously) provided by the data subjects; while personal data that data controllers "observe" are not disclosed by individuals in an explicit manner, but, e.g., obtained through cookies, GPS, simple combination of raw data, etc.

The above-mentioned restrictive interpretation includes only "received data" in the definition of "data provided to the controller"; while the extensive one includes both "received" and "observed" data, while the expression "provided" seems more limited.

For both these options, there are possible arguments and counterarguments.

The restrictive interpretation should be adopted first of all for a "semantic" reason: "providing" is an active task and it is different from "accepting that someone takes my data" e.g., through cookies, GPS, metadata, etc. (passive).[40] Indeed, in other parts of the GDPR "passive" forms are used to refer to the storing of personal data, which may be interpreted extensively, e.g., Article 15(g) mentions "data (. . .) collected from the data subject". The expression "data *collected* from the subject" can indeed well refer both to "received" data and to "observed" data.

It is also true that considering the increasing use of intrusive data-retrieval technologies, providing consent (i.e., "accepting that someone takes my data") might be one of the few things that users will be asked to do in the future. In other words, nearly all data obtained from data subjects will be "observed" data.

Another argument in favour of the restrictive interpretation is the concrete (un)feasibility for data controllers to comply with a wide right to data portability. It may be indeed argued that transmitting to the individuals all data pertaining them (also metadata, location data, etc.) may be in some specific cases unreasonably expensive for data controllers. However, even assuming that these unreasonable costs of data portability might exist in concrete, they should be fully demonstrable by data controllers. At the same time, if such expenses would be so heavy so as to threaten the right to conduct a business, there is already a general balancing clause (Article 20(4)), clarifying that the portability right should not adversely affect rights and freedoms of others. In other words, if the extensive interpretation of "data provided" could in theory substantially damage the freedom to conduct a business of data controllers, the judicial application of the balancing clause in Article 20(4) should avoid that in a specific case the application of right to data portability will adversely affect interests of data controllers.

In favour of the restrictive interpretation, there are also some scholars who have already highlighted that the right to data

[37] See J. VERSCHAKELEN and P. VALCKE, *Putting the Right to Data Portability into a Competition Law Perspective*, et al., p. 63: "Because of uncertainty about the interpretation of some of its key terms, the exact scope of application of the right to data portability is still unclear". Also "Centre National Informatique et Liberté" (CNIL) in a public consultation about new GDPR highlighted the problematic object of right to data portability: see https://www.cnil.fr/sites/default/files/atoms/files/resultats_de_la_consultation_publique_reglement_0.pdf (accessed 30 May 2017). See also Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*, supra, p. 2 arguing that organisations need to have full legal certainty about the scope of application of the data portability right, as envisaged in the GDPR, in order to be able to make the appropriate changes and investments and not to be required to 'reinvent the wheel later on".

[38] See G. MALGIERI, Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, Privacy in Germany - PinG, n. 4, 2016, p.133 ff., 143. See also B. VAN DER AUWERMEULEN, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, Computer Law & Security Review 33 (2017), 57–72, p. 61. See, contra, Article 29 WP, *Guidelines*, supra, p. 10, which includes in the balancing clause at Article 20(4) also the protection of intellectual property and trade secrets of data controller, in particular through the application of recital 63 (referring to the right to access of Article 15) in the field of data portability.

[39] See G. MALGIERI, Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, supra.

[40] See also Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*, 15 February 2017, p. 8 highlighting the need of a "voluntary, affirmative element of 'providing' data to the controller, as opposed to collecting data from an individual who may be passive".

portability should include directly uploaded data (e.g., photos and information a user has typed into a site, such as status updates or profile information); while other data should not fall within the definition.[41] In particular, it has been argued that "observed data" is a too wide category, where also technical analyses may be included e.g., in the field of 'network traffic data'.[42] However, they are at the same time quite uncertain about "metadata" inclusion within the object of portability right.[43]

As regards the extensive interpretation, the biggest argument in favour of it is found in recital 68. There it is clarified that "the right to data portability should apply *where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract*".

It seems, thus, clear that not only data explicitly provided in a written format could be the object of portability, but also all data provided on the basis of data subject's consent or within the performance of a contract, meaning therefore also cookies and GPS data (since users provide their consent for their collection).

It might be also answered that recital 68 is only clarifying that data which is given on other legitimate grounds other than consent or contract (e.g., legal obligation, legitimate interests, public interests, etc.)[44] cannot be included in the scope of this new right to data portability, as also Article 20(3) states.

Recital 68 also provides – as mentioned above – that the right to data portability has the purpose of "further strengthen[ing] the control of [data subjects] on their own data". Consequently, only the extensive interpretation (since "data subjects friendly") can really strengthen the control rights of data subjects on their own data. It has also been argued that when dealing with human rights of individuals in the technological field the interpretation more in favour of individuals should be always preferred.[45] For all these reasons, "provided data" should mean *all data which have not been processed through an intellectual activity of the controller*, but including not only data explicitly disclosed in a written form (or similar) to the controller, but all data just "observed" by the controller (e.g., location data, fitness data,[46] etc.) without any further (intellectual, economic, and scientific) effort from the controller (e.g., algorithmic results).

Moreover, WP29 has recently approved the extensive approach. It clearly states that the phrase "*provided by*" must be interpreted broadly, so as to include "personal data that relate to the data subject activity or result from the *observation of an individual's behaviour* but not subsequent analysis of that behaviour. By contrast, any personal data which has been generated by the data controller as part of the data processing, e.g., by a personalisation or recommendation process, by user categorisation or profiling is data which is derived or inferred from the personal data provided by the data subject, and is not covered by the right to data portability".[47]

The EDPS had also recommended that, in order to be effective, the right to data portability should have "a wide scope of application, and not only be applied to the processing operations that use data provided by the data subject".[48]

Obviously, the interpretation proposed here should be based on a case-by-case approach; therefore, only Courts will be able to resolve "grey" areas (e.g., data which are neither fully "observed", nor totally "inferred" by data controllers) in the first applications of the GDPR.

5. Impact of data portability

The impact of a right to data portability is relevant both for businesses (in particular for e-businesses involved in the digital market, e.g., internet service providers) and for individual users (data subjects). From the *business perspective*, this impact is tangible in several fields: it is both a challenge to the traditional system of *competition law*[49] and a 'problematic opportunity' in terms of *interoperability* of systems. From the *user perspective*, the impact of data portability is evident both in terms of *control* of personal data (and in general in the sense of empowerment of control rights of individuals), and in terms of a more user-centric interrelation between services. At the same time, it is a challenge to third data subjects' rights.

As regards *interoperability* of systems, recital 68 of the GDPR states that data controllers "should be encouraged to develop interoperable formats that enable data portability". Therefore, efforts imposed upon data controllers towards a fully interoperability of digital systems are moderate: they "should be encouraged" and not obliged to develop these "interoperable formats".

---

[41] P. SWIRE and Y. LAGOS, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy, Critique Public Law and Legal Theory Working, Paper Series No. 204, May 31, 2013, 347.

[42] Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"*, supra, p. 8 which – however – recognizes also that some "observed data" are clearly within the scope of "provided data", e.g., in the field of wearable tracking devices "where the individuals willingly and knowingly provide tracking data and sensed data because it is part of the desired service to the individual and conveys a desired benefit to the individual".

[43] *Ibidem*.

[44] See Article 6, GDPR.

[45] P. DE HERT, The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us, EDPL, 2016/4.

[46] Article 29 WP, *Guidelines*, rev01, supra, p.10: "They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by fitness or health trackers" and also "transaction history and access log" (see footnote 12).

[47] "Article 29 WP, *Guidelines*, rev01, supra, pp. 10–11. See also Article 29 Working Party Issues Results of Fablab Workshop on the GDPR.

[48] EDPS recommendations on the EU's options for data protection reform, (2015/C 301/01).

[49] See I. GRAEF, J. VERSCHAKELEN and P. VALCKE, *Putting the Right to Data Portability into a Competition Law Perspective* (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53–63, 63. See also Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*, p. 2, which argues that an overbroad implementation of the data portability right may stifle competition and innovation and impose unnecessary burdens on organisations. Actually, according to others, "site owners have an economic interest to support the portability of people's data", which is based on the increasing of trust, see E. BIZANNES, 'Why Every Site Should Have Data Portability Policy' (Techcrunch, 23 June 2010) http://techcrunch.com/2010/06/23/data-portability-policy/ (accessed 28 February 2016).

A further confirmation of this is the final part of recital 68: data subjects "should have the right to have the personal data transmitted directly from one controller to another", but only "*where technically feasible*".[50] In other words, data controllers can prevent a full exercise of users' right to data portability if they prove that in a given situation the level of technological development of their organisation makes technically unfeasible a direct transmission of data to another controller, e.g., because interoperable formats (encouraged, but not imposed) have not yet been developed.[51]

At the same time, in the final adopted version of the GDPR there is no obligation (in terms of deadlines and effort) to reach a system of interoperability in the future. Actually, as clarified above, in the first proposal of the European Commission, Article 18(3) stated that the Commission could "specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2"; therefore it would have imposed and monitored concrete efforts and steps towards an effective system of interoperability between digital services.

Unfortunately, this provision has been removed from the final version, thus revealing a more prudent approach of the European legislator towards businesses concerns.

On the other hand, as regards the empowerment of data subjects, recital 68 of GDPR explains that the rationale of right to data portability is to "*further strengthen the control* [of the data subject] over *his or her own* data".

In other terms, right to data portability is conceived as a means to empower control of individuals on personal data.[52] What is interesting in that sentence of recital 68 is the reference to "*his* or *her own* data": in general, when EU Data Protection law (i.e., both the Data Protection Directive and the GDPR) mentions the relationship between personal data and data subjects it uses the expression "data relating to him or her" (or "to the data subject").[53]

For the first time, here, the expression used is "*his* or *her own* data". It is also echoed by recital 7: "Natural persons should have *control* of *their own personal* data". Furthermore, here the reference to "*own* data" is related to the idea of controllership. Right to data portability is therefore an essential element towards empowerment of data subjects and a first step to an idea of data subjects' default *own*ership of their personal data.

6. Relationship with the rights to access and erasure

Another aspect that appears as a possible issue is the interrelation between right to data portability and other "control rights" of data subjects on their personal data. In particular, the *right to access* and the *right to erasure* (or to be forgotten) should be compared to right to portability. The first, because it can create an overlap with data portability; and the second, because its interplay and balancing with the right to data portability may be problematic. As for the *right to access*, it is substantially different from the right to data portability. In principle, it could be held that the first is a right of "knowledge", while the second is a right of "controllership".

On the one hand, right to access (Article 15) is much wider as regards the scope of the right: it is not only about "*data provided* by consumers", but it refers also to: (a) the *purposes* of the processing; (b) the *categories* of personal data concerned; (c) *the recipients* to whom the personal data has been or will be disclosed; (d) *the envisaged period* for which the personal data will be stored; (e,f) the existence of other data subject's rights; (g) any available information as to the source of data; and (h) the *existence of automated decision-making*, including profiling, and *meaningful information about the logic involved*, as well as the *significance and the envisaged consequences* of such processing for the data subject. In addition, reaction powers of individuals in the right to data portability are much wider. Indeed, data subjects can: 1) receive data in a workable format (Article 20(1)); 2) transmit this data to another controller (Article 20(1)); and 3) have the personal data transmitted directly from one controller to another (Article 20(2)).

In principle, "access" is different from "obtaining". Accordingly, what is relevant in data portability is the machine-readable format of data; while in the right to access, there is no duty to provide data in a workable format.

As regards the *right to erasure*, Article 20 of the GDPR states that the exercise of the right to data portability shall be without prejudice to Article 17 (i.e., the right to erasure). We have already addressed *supra* the analysis of balancing clauses in Article 20.

What is, however, interesting is that in the (non)interplay between the right to erasure and the right to be forgotten there might be a great development of data portability potentialities. To be clearer, recital 68 explains that the right to data portability "should, in particular, *not imply the erasure of personal data concerning the data subject which has been provided by him or her* for the performance of a contract to the extent that and for as long as the personal data is necessary for the performance of that contract".

Actually, in the first Commission proposal there was a reference to "the controller from whom the personal data is *withdrawn*", but – as explained above – this formulation has been removed in the approved version. Thus, the right to data

[50] *Ibidem*, p. 62, according to whom the formulation "when technically feasible" appears "too permissive".

[51] For what regards this specific example we need to clarify that many interoperable formats already exist, what is often missing are the interoperable interfaces that can "use" them (import and export). In addition, while the usage of these interoperable formats could provide syntactic interoperability, semantic interoperability is much harder to achieve and might only be feasible between data controllers that manage data of the same nature.

[52] See, however, Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*, 15 February 2017, p. 2, which highlights that in some fields portability of data would not be an empowerment for individuals, e.g., in respect of employees' data or personal data in the context of B2B activities. Moreover, "in the consumer contest there might be circumstances where porting data would not necessarily be in the interest of the individual because the receiving controller may not use the ported data for the same purpose or because an excessive amount of data would be overwhelming to the individual".

[53] See, e.g., Article 2(a) and (h), , Article 10, Article 12(a), Article 14(a) and (b), Article 15(1) of the Data Protection Directive, 95/46/EC and also recitals 32, 58, and 61 and Article 4(1) and (11), and Article 13, GDPR.

Table 1 – Comparison between restrictive and extensive approach to data portability.

	Restrictive approach	Extensive approach
"Data provided"	Only data explicitly provided by data subjects	All data accessible by data controllers
Relationship with the right to erasure or withdrawal of data	Close (the exercise of data portability is inherently linked to the withdrawal/erasure of data from the first data controller)	Indirect (data portability does not automatically imply the erasure of data from the first data controller)
Scenarios	*Adieu scenario* (data are ported from service X to service Y)	*Fusing scenario* (data portability encourages the creation of platforms of interoperable services)

portability cannot be considered a mere right to transfer data from one controller to another one, asking simultaneously the first controller to erase such data.

Instead, it is an opportunity for data subjects to transmit their data to, e.g., new service providers, and only in case they want to withdraw such data from the first data controller's databases, they should exercise another separate right (*right to erasure*) which has different (wider) exercisability requirements and a different legal basis.

In other words, the EU legislator did not want the exercise of data portability to include the simultaneous withdrawal of data from the first controller.[54] On the contrary, if we read that provision jointly with the emphasis on "the encouragement towards interoperability" of formats (and services)[55] and the new right "to have the personal data transmitted directly from one controller to another" we can understand that the intention as adopted in the GDPR is not a mere transfer of personal data, but the development of a solid (and possibly user-centred) interconnection between different digital services.

7. Possible scenarios: potentialities of data portability

Moving from the just-mentioned reflections about the simultaneous exercise of the right to data portability and the right to erasure we can summarise two opposite approaches to data portability.

This new right permits only the transfer of "provided" personal data from one service provider to another. The passage from one digital service provider to another is made easier by the possibility of "removing" customers' data from the first provider, while transferring it to the new one. We call this approach the ***adieu scenario***.

Alternatively, right to data portability may be seen as the valuable opportunity for an effective development of a user-centric platform where all digital services are interconnected.[56] Users can create an account and export their account data to other digital services,[57] including their "Quantified Self" data (i.e., lifestyle data), nicknames, their intellectual creations (e.g., virtual properties in virtual worlds), all user generated content, etc. We call this approach the ***fusing scenario***.

In other words, the right to data portability should be the stimulus capable to turn the fragmented multiplicity of digital services into interoperable segments of a user-centric Internet of things.

Accordingly, the right to data portability should not be necessarily based on the simultaneous erasure of data from the first data controller, but on the addition of a new data controller for new potential processing purposes.

This scenario does not only encourage a real competition between service providers (limiting barriers for users willing to change service in the digital market),[58] but it also avoids the monopolisation of the Internet by large companies, by encouraging interoperable formats, developing multilevel platforms where the centre is the user and the actors are different service providers. There are already several experimental applications in Europe of these new platforms.[59]

These two scenarios correspond to the two different interpretations of "data provided" as outlined above (see Table 1).

[54] See also Article 29 WP, *Guidelines on the right to data portability*, supra, p. 17.

[55] See recital 68, "data controllers should be encouraged to develop interoperable formats that enable data portability".

[56] See Article 29 WP, *Guidelines on the right to data portability*, rev01, supra, p. 3. See also the criticisms of S. WEISS, 'Privacy threat model for data portability in social networks applications', (2009) 29, International Journal of Information Management 249 ff., 250, according to whom data portability may increase the complexity of control and process of personal data.

[57] A model of users directly exporting data is the "pull model" proposed in Centre for Information Policy Leadership, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"*, supra, p. 4. Actually this proposal has a minimalist approach, given that it does not go towards a development of user-centric interoperable formats, but it just suggests a practical (and minimal) way to deal with the right of individuals to transmit personal data from one data controller to another.

[58] See D. GERADIN and M. KUSCHEWSKY, *Competition Law and Personal Data: Preliminary thoughts on a Complex Issue*, 12 February 2013, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216088 (accessed 31 January 2017). See also B. VAN DER AUWERMEULEN, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, Computer Law & Security Review 33 (2017), 57–72, who compares the applicability of EU Competition Law to data portability with the US competition rules.

[59] See, e.g., MiData in the United Kingdom, MesInfos/SelfData by FING in France, etc.

Indeed, the restrictive approach (i.e., only data explicitly given by users can be ported) is more compatible with the *adieu scenario*, where there is a mere transfer of account data from digital service X to digital service Y. On the other hand, the extensive approach (i.e., all "observed" data can be ported) better allows a full development of the *fusing scenario*.

In a user-friendly interconnection of services, the more personal data are shared, the more users will benefit from it.[60] As it has been argued, data portability is the ability for people to *reuse* their data across devices and services.[61] This new right should transform passive data subjects into active reusers.[62] Indeed, it should empower consumers to take advantage of value-added services from third parties and lets them "share the wealth" created by big data.[63]

8. Concluding remarks

The right to data portability is one of the most remarkable novelties of the GDPR. Its impact is particularly relevant both on data economy and on control rights of individuals.

On the one hand, it can be the opportunity to foster interoperability of services, increase competition between digital services and develop more and more user-centric platforms for the management of personal data.[64] On the other hand, it represents the first theoretical step towards a default ownership of personal data to data subjects.

Several points are still challenging: the role of European Commission in incentivising interoperability has been removed from the first proposal of GDPR: the object of data portability is still unclear and likely to have a too restrictive interpretation; the efforts required towards the development of interoperable formats and interfaces to port data are minimum; and a very prudent balancing structure has been chosen.

Thus, the actual text of the GDPR allows two opposite options: a minimum approach, where the object of data portability is only data explicitly given to the controller (e.g., in a written form) and where right to data portability is inherently linked to the withdrawal of data from the first controller (an "adieu" scenario); or an extensive approach, where a wide interpretation of "data provided" (including also data observed by the controllers) joined with the right to have data directly transferred from one controller to another (Article 20(2)) allows a "fusing" scenario, towards user-centric platforms of interrelated services.

What we propose here is to adopt the latter, extensive, approach considering that the rationale of this right (recital 63) is to "further strengthen control rights of the data subject on his or her own data" and "foster opportunities for innovation by means of sharing of personal data between data controllers in a secure manner under the constant control of the data subject".[65]

[60] See Article 29 WP, opinion 03/2013 on purpose limitation, WP 203, p. 47.

[61] B. CUSTERS and H. URSIC, Data Reuse, supra, 8, see also D. GERADIN, 'Data Portability and EU Competition Law', BITS conference, Brussels 2014.

[62] B. CUSTERS and H. URSIC, Data Reuse, supra, 9.

[63] Article 29 WP, Opinion 3/2013, supra.

[64] EDPS, Opinion 9/2016 on Personal Information Management Systems -Towards more user empowerment in managing and processing personal data, 20 October 2016.

[65] Article 29 WP, *Guidelines*, rev01, p. 5.