II. The Right to Data Portability

A. Brief Overview on the GDPR

Already in 2010, the Commission laid down the foundations for the ambitious modernization of the EU's personal data protection framework,[17] which culminated in the GDPR's enactment. It was the result of extensive reviews, consultations and studies, concluding that legislation then in place (in particular, the Data Protection Directive (DPD)[18]) could no longer cope with the new challenges emerging from technology development and globalization.[19]

The digital age changed both the economy and society, and opened a new world of possibilities for data collection, processing, storage, sharing and analysis.[20] While individuals undoubtfully benefited from new products and services, their use came intertwined with a high price in terms of data protection. The consequence was a loss of control and trust in the online environment, which the Commission considered as one of the main obstacles for the EU's digital single market strategy.[21]

Distrust in digital products and services has a direct impact on the EU's economic development. Consumer lack of confidence can prevent adoption of new digital products and services, leading to a disincentive to innovate.[22] In view of this, the Commission acknowledged the strengthening of

---

17 Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM(2010) 609 final.

18 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive – DPD).

19 COM(2010) 609 final (n 17) 5.

20 Commission, 'Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data' (Commission Staff Working Paper) SEC(2012) 72 final 7.

21 Ibid 7, 22-5.

22 Ibid 7.

individuals' rights (in particular, control over their own data) as one of the reform's key objectives.[23]

The GDPR's material scope consists of the processing of personal data (further discussed below).[24] Its territorial scope provides for a far-reaching provision: it applies to processing conducted within the context of an establishment in the EU/European Economic Area (EEA),[25] as well as cases where the establishment is outside but the processing relates to a data subject within the EU/EEA, to whom the goods or services are being offered, or whose behaviour is being monitored.[26]

Starting with the choice of secondary law,[27] to the introduction of new rights of data subjects, the GDPR is considered by many as a truly innovative and revolutionary piece of legislation.[28] The catalogue of data subjects' rights was complemented with two new ones: (i) the right to erasure (or, as commonly known, right to be forgotten),[29] and (ii) the RtDP.[30] While the former had already been recognized by the Court of Justice of the European Union (CJEU),[31] the latter has no predecessor in the realm of EU data protection law.

But before analysing the RtDP, the concept of 'personal data' has to be discussed in detail, as it is vital to determine the RtDP's scope.

---

23 COM(2010) 609 final (n 17) 5.

24 GDPR art 2(1). Article 4(2) defines 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means', while Article 2(2) excludes certain types of processing from the GDPR's scope.

25 GDPR art 3(1).

26 GDPR art 3(2)(a)-(b).

27 Under the DPD, significant divergences were verified across Member States' national data protection laws. To ensure a level playing field for the data economy, the Commission opted for a regulation. COM(2010) 609 final (n 17) 3; SEC(2012) 72 final (n 20) 11.

28 Carolina Banda, *Enforcing Data Portability in the Context of EU Competition Law and the GDPR* (Master Thesis, MIPLC 2017) 61, 28; Graef, Husovec and Purtova (n 7) 2; Gabriela Zanfir, 'The right to Data Portability in the Context of the EU Data Protection Reform' (2012) 2 IDPL 149, 150.

29 GDPR art 17.

30 GDPR art 20.

31 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.

B. The Concept of 'Personal Data'

Article 4(1) GDPR defines 'personal data' as 'any information relating to an identified or identifiable natural person', the so-called 'data subject'. It further specifies that an 'identifiable natural person' is in place where she 'can be identified, directly or indirectly'. Besides obvious identifiers, such as name and ID, the definition lists 'location data, an online identifier or (…) factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity' as additional examples.[32]

The CJEU adopted a quite broad interpretation of the definition, especially concerning 'identifiability'.[33] In 2011, the Court held that an IP address could be personal data from an Internet Service Provider's (ISP) perspective.[34] Later, it clarified in *Breyer* that even a dynamic IP address could constitute personal data, where the controller would have the means to obtain additional information to identify the data subject.[35]

In line with the case-law, Recital 26 GDPR provides further guidance by adopting a 'test of reasonable likelihood of identification'.[36] All means reasonably likely to be used by the controller or a third party must be considered. How costly and time consuming the means are, as well as the technology available at the time of processing, have to be considered to establish identifiability.

More recently, the CJEU ruled in *Nowak* that even written answers of a candidate's exam and the examiner's comments thereto are 'personal data'.[37] It held that

> [T]he expression 'any information' (…) reflects the aim of the EU legislature to assign a wide scope to that concept [of personal data], which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective.[38]

---

32 Articles 4(13)-(15) GDPR further define three special categories of personal data: (i) genetic data; (ii) biometric data; and (iii) data concerning health.

33 Although case-law is still based on the DPD, considering the similarity of the provisions, the principles carry across.

34 Case C-70/10 *Scarlet Extended* [2011] ECLI:EU:C:2011:771 para 51.

35 Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779 paras 44-49.

36 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) LIT 40, 44.

37 Case C-434/16 *Nowak* [2017] ECLI:EU:C:2017:994 para 62.

38 Ibid para 34.

Taking account of the above, 'personal data' might encompass any kind of information, even non-personal and pseudonymized data[39] that, when combined with some additional data, can identify the individual.[40] Contrarily, anonymous data, ie 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable',[41] falls outside the scope.

This leads to a very broad and context-dependent definition.[42] The main issue is the difficulty of setting a clear borderline between personal and non-personal data, which is essential for determining the GDPR's scope. This holds especially true with current improvement and exponential use of powerful data analytics.[43] Combination of constantly growing datasets and the fast development of (re)identification technologies results in a higher likelihood of two remote pieces of information culminating in identifiability.[44]

To better understand the dimension of such broad definition, take the Commission's example – home temperature sensors.[45] In a first hint, one would probably not relate data collected by such devices to personal data. However, home temperature will be considered personal data if there is a reasonable likelihood that it could be linked to a natural person. Their sensors can collect personal and non-personal data.

---

39 Article 4(5) GDPR defines 'pseudonymisation' as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

40 Recital 26 GDPR states that 'personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person'.

41 GDPR rec 26.

42 Purtova (n 36) 47.

43 Josef Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' (2018) BEUC <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 9 June 2019, 48; Graef, Husovec and Purtova (n 7) 8.

44 Drexl, 'BEUC Study' (n 43) 48; Purtova (n 36) 41-2, 47.

45 COM(2017) 9 final (n 2) 9.

Hence, it is necessary to set bias on personal data aside and keep an open mind. The world has changed with technology, as does the concept of personal data.

C. The Right to Data Portability under the GDPR

Article 20 GDPR introduces an entirely novel right – the RtDP – which is considered a major legal innovation. As a personal right, only the concerned (living) data subject has a claim under the RtDP.[46] Although it is comparable to the telecom's number portability,[47] it is concomitantly something completely different, as discussed below.

1. Legislative History and Purpose

Complementing the rights of data subjects with a portability right was within the Commission's plans from the very beginning,[48] as it reported to have received queries from several individuals complaining that they were unable to retrieve their personal data from online service providers.[49]

An individual's increasing dependence on online services and the inability to easily retrieve their personal data therefrom results in high switching cost. Time and effort to change might be so burdensome, that users decide to stay with the current provider, even if better ones are available on the market.[50] This scenario is referred to as a 'lock-in effect'.

To ensure improvement on individuals' control, withdrawal from their personal data from one application or service and transfer into another one, was considered essential. The European Data Protection Supervisor (EDPS) considered the RtDP as a strategic element, a 'gateway in the digital environment to the user control which individuals are now realizing

46 According to Veil, the claim may also be asserted by a legal representative (eg a lawyer or legal guardian). Winfried Veil, 'Artikel 20 – Recht auf Datenübertragbarkeit' in Gierschmann S and others, *Kommentar Datenschutzgrundverordnung* (Bundesanzeiger 2018) 590, 600-1.
47 SEC(2012) 72 final (n 20) 28.
48 COM(2010) 609 final (n 17) 8.
49 Ibid 7.
50 SEC(2012) 72 final (n 20) 28.

they lack'.[51] Online platforms,[52] especially social networks,[53] have always been the Commission's focus. Notwithstanding the (attempted) tailoring for online platforms, the final wording is neutral, not confining its applicability to any specific sector.

The Commission's 2012 proposal for the GDPR first introduced the RtDP as an independent right under Article 18.[54] Thereafter, the European Parliament's review included it under Article 15(2a) regarding the right to access.[55] This merger was perceived as the Parliament's way of expressing its view that the RtDP is an extension of the right to access.[56] However, after discussions in the Council, the RtDP was assigned once again an independent article in the final version.[57]

During review in the Council, several delegations expressed concerns about including the RtDP in the GDPR.[58] One of the main reasons was that the RtDP could be more a matter of competition law or consumer law, rather than of data protection. As discussed, consumer lock-in was a core issue, which can represent a market entrance barrier in detriment of consumer welfare.[59]

In view of the above, it is possible to differentiate the RtDP's purpose from its rationale. While the purpose of the RtDP is to strengthen data subjects' control and build trust in the digital environment, the underlying rationale is to avoid lock-in. It is therefore recognized, that the RtDP has

51 EDPS, 'EDPS Recommendations on the EU's Options for Data Protection Reform' [2015] OJ C 301/1, 5 (item 3.2).
52 The concept of 'online platform' includes search engines, social networks and e-commerce platforms. Graef, *Essential Facility* (n 6) 16.
53 COM(2010) 609 final (n 17) 7.
54 Commission, '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) 11 final, 9, 53.
55 European Parliament, 'Report 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)' A7-0402/2013, amendment 111.
56 Graef, Husovec and Purtova (n 7) 4.
57 GDPR art 20.
58 Council Doc ST 10614 2014 INIT (06.06.2014) 3, fn 1.
59 Barbara Engels, 'Data Portability Among Online Platforms' (2016) 5 (2) IPR 5.

concomitantly a data protection, consumer law and competition law dimension.[60]

2. Scope of the Right to Data Portability

The scope of the RtDP vests data subjects with a two-folded right: (i) a right to receive and transfer personal data[61] (indirect portability), and (ii) a right to have it transmitted directly from one controller to another[62] (direct portability).[63]

Article 20(3) GDPR clarifies that the RtDP is without prejudice to the right to erasure. Accordingly, after completion of a portability, the data subject's personal data will be both with the first controller and the data subject and/or the second controller.[64] In this regard, the RtDP differs significantly from the telecom number portability, where the first service provider does not retain the individual's number after portability conclusion. Considering such characteristic, the RtDP could arguably be a right of 'copying' or 'sharing' one's own personal data.

The indirect portability is also two-folded – it grants data subjects a right (i) to receive their personal data, and (ii) to transmit them to another controller without hindrance from the original controller. The controller has to provide the data 'in a structured, commonly used and machine-readable format', which is not defined in the GDPR. Recital 68 adds that the format should be interoperable.

The rationale of the format requirement can be inferred from the Commission's proposal – it should allow 'for further use [of the data] by the data subject'.[65] They are minimum requirements to enable reuse of the data by the individual or another controller.[66]

---

60 Inge Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' (2016) <https://ssrn.com/abstract=2881969> accessed 15 March 2018, 10.

61 GDPR art 20(1).

62 GDPR art 20(2).

63 Hans-Georg Kamann and Martin Braun, 'Art. 20 Recht auf Datenübertragbarkeit' in Ehmann E and Selmayr M (eds) *Datenschutz-Grundverordnung: DS-GVO* (2nd edn, Beck 2018) 495, 502-05; Veil (n 46) 614.

64 Veil (n 46) 614.

65 COM(2012) 11 final (n 54) art 18(1).

66 WP242 (n 14) 17.

As argued by Veil, the expression 'structured format' is probably incorrect.[67] It is not the format in which the personal data is transferred that has to be structured, but rather the data itself. This seems indeed more in line with the objective of data reuse.

Considering the RtDP's applicability across sectors, the commonly used format requirement seems the most complex one to achieve, as different standards apply to different sectors.[68] Suggestions were made regarding sector-specific standards for compliance with the provision, but this would not solve the issue when portability is requested across sectors. Thus, the preferred approach would be to understand it as requiring controllers to use a format compatible with the state-of-the-art when of the portability request.[69] This would not prevent, however, adoption of sector-specific regulations where appropriate.

With regard to the machine-readable format requirement, recourse can be taken from Directive 2013/37/EU, which 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'.[70] The provision clarifies that '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'. A PDF file, for instance, was not considered machine-readable by WP29.[71]

Furthermore, the data subject has the right to transmit her personal data to another controller *without hindrance* from the first controller. According to the WP29 Guidelines, a hindrance is 'any legal, technical or financial obstacles placed by data controller to refrain or slow down access, transmission or reuse by the data subject or by another data controller'.[72]

67 Veil (n 46) 612.

68 Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 MdLRev 335, 346. Drexl, 'BEUC Study' (n 43) 109 even argues that if such commonly used formats do not exist, the data subject will have no claim under the RtDP. Applicability of such a strict interpretation seems aligned with the technical feasibility requirement for direct portability, but would probably not justify a refusal in case of indirect portability.

69 Kamann and Braun (n 63) 503.

70 Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance [2013] OJ L 175/1, rec 21.

71 WP242 (n 14) 18.

72 Ibid 15.

Direct portability is subject to an additional condition – only where it is 'technically feasible' will there be an obligation to comply with a request. Once again, the GDPR falls short, not providing for a definition or explanation.

A basic requirement is that the transmitting and receiving data processing systems be able to communicate, ie be interoperable. However, Recital 68 GDPR solely states that the RtDP 'should not create an obligation for controllers to adopt or maintain processing systems which are technically compatible'. As highlighted by Scudiero, direct portability will extremely 'depend on the availability of standards that make different systems interoperable',[73] which holds true especially considering the RtDP's applicability across sectors.

The likelihood of controllers refusing to comply with portability requests based on technical unfeasibility cannot be underestimated.[74] Although Recital 68 GDPR encourages the development of interoperable formats, there is no legal obligation. In cases where the controller is unwilling to share the individual's personal data with a third party this might seem a good way to circumvent the obligation, undermining the RtDP's purpose.[75]

It is still uncertain in which cases a controller will be able to refuse direct portability based on technical unfeasibility. WP29 understands the 'technical feasibility' concept as (i) a secured communication system between the transferring and receiving controllers, as well as (ii) the capability of the receiving controller's system to receive the incoming data.[76] Nevertheless, it is noteworthy that the GDPR does not oblige the target controller of a portability request to accept the transferred data.[77]

What is technically feasible in practice also depends on the controller's size and sector. What might be technically feasible for big tech giants, might not be for Small and Medium Enterprises (SMEs).[78] It accords with

73 Lucio Scudiero, 'Bringing Your Data Everywhere: A Legal Reading of the Right to Portability' (2017) 3 (1) ECPL 119, 124.
74 Vanberg and Ünver (n 6) 4.
75 Ibid 2.
76 WP242 (n 14) 16.
77 Drexl, 'BEUC Study' (n 43) 109, 147; Kamann and Braun (n 63) 505; Veil (n 46) 603-04; WP242 (n 14) 6.
78 Ruth Janal, 'Data Portability - A Tale of Two Concepts' (2017) 8 (1) JIPITEC 59, 5; Vanberg and Ünver (n 6) 4.

WP29's recommendation to assess technical feasibility on a case-by-case basis.[79]

In any event, even in cases of technical unfeasibility, the data subject still has the right to indirect portability and nothing prevents her from subsequently transferring it to another controller. However, this obviously does not favour reduction of consumers' switching costs.

Furthermore, Drexl argues that the RtDP's exercise should not be limited to *ex-post* situations, ie only after personal data provision.[80] The data subject should be able to request portability also for future data, whereby every new piece of data is automatically sent from the transferring to the receiving controller.[81] This would undoubtfully provide for even stronger control and better reuse of individuals' data, but will ultimately depend on case-law to support it as a right, not merely as a voluntary act of controllers.

3. Conditions for the Right to Data Portability

The RtDP is subject to three cumulative conditions: (i) processing must be based on consent of the data subject or a contract;[82] (ii) the form of processing must be by automated means; and (iii) the object of the processing must be personal data provided by and concerning the data subject.[83]

If any condition is not met, the RtDP cannot be invoked. Thus, each condition will be analysed in the subsections below:

(a) Processing Based on Consent or Contract

Solely processing of personal data based on (i) the data subject's consent, or (ii) a contract between the data subject and the transferring controller, is subject to the RtDP.[84] Data processed on any other legal ground (includ-

79 WP242 (n 14) 16.
80 Drexl, 'BEUC Study' (n 43) 110.
81 Some social networks already provide for this possibility. For instance, when posting a photo on Instagram, the user can opt to automatically share it on Facebook, if both accounts are linked.
82 GDPR art 6(1)(a) (general consent), 9(2)(a) (special categories of data), 6(1)(b) (contract).
83 GDPR art 20(1).
84 GDPR art 20(1)(a).

ing legitimate interest under Article 6(1)(f) GDPR), as well as 'processing necessary for performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'[85] are excluded from the RtDP's applicability.

Notwithstanding such limitation, WP29 recommends personal data portability to be adopted as a good practice, even in non-mandatory cases.[86] This will be particularly important for borderline cases, such as employment relations, where the employer generally processes employees' personal data based on legitimate interest,[87] albeit the existence of an employment contract.

Although the idea was to exclude other *lawful* processing grounds, the broad wording also leaves *unlawfully* processed data outside the RtDP's scope.[88] This leads to a situation where the data subject, besides having been subject to an illegal data processing, will not be able to retrieve her data from the controller. In view of this, it is recommended that the RtDP also applies where the individual did not consent.[89]

(b) Processing by Automated Means

The RtDP has a more limited applicability if compared to the GDPR's scope, which also applies for 'processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'.[90] Under Article 20(1)(b) GDPR, the RtDP applies only where the processing is 'carried out by automated means'.

As the GDPR lacks a definition of 'automated means', the only straight forward interpretation is that non-automated means are excluded. Recital 15 provides further guidance, indicating that it does not encompass manual processing, ie processing conducted by an individual. This also seems to be the understanding of WP29, as paper files were deemed excluded.[91]

---

85 GDPR rec 68, art 20(3).
86 WP242 (n 14) 8, fn 16.
87 Helena Ursic, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) SCRIPT-ed (forthcoming) <https://ssrn.com/abstract=3176820> accessed 29 June 2018, 16; WP242 (n 14) 8-9.
88 Drexl, 'BEUC Study' (n 43) 152-53; Janal (n 78) 3-4.
89 Ibid.
90 GDPR art 2(1).
91 WP242 (n 14) 9.

Under its ordinary meaning, 'automated' is something operable by machines or computers. Most scholars adopt this path, as the expression is referred to as processing 'by a computer',[92] 'through technology',[93] or using 'data processing systems'.[94] Commonly listed examples include social networks, cloud computing, web services, and smartphone apps.[95] It is also in line with the original proposal, which refers to processing 'by electronic means'.[96]

Furthermore, as the GDPR applies to processing of personal data both wholly or partly by automated means,[97] it remains unclear if this is also the case for the RtDP. One could read the absence of a qualifying adverb (as opposed to the express reference under other provisions[98]), as an indication that the RtDP also applies to partially automated means.[99] Such broader interpretation would be consistent with the RtDP's objective of strengthening individual's control over her data.

However, considering the '*machine-readable format*' requirement,[100] the argument for requiring the process to be conducted wholly by automated means seems more coherent. Should the processing be carried out partially by automated means, the controller would first have to transform the relevant data into a machine-readable format, which represents an additional step and burden.

(c) Personal Data 'Concerning' and 'Provided by' the Data Subject

Article 20(1) GDPR determines that the RtDP is limited to personal data concerning the data subject making the request. This means, *first*, that only

92 Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' [2017] <https://ssrn.com/abstract=2933448> accessed 28 March 2018, 3.
93 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 383, 10.
94 Ibid 170; Zanfir (n 28) 158.
95 See Swire and Lagos (n 68) 338; Vanber and Ünver (n 6) 2.
96 COM(2012) 11 final (n 54) art 18(1).
97 GDPR art 2(1).
98 For instance, see Article 22(1) GDPR, which refers to a 'decision based *solely* on automated processing'.
99 Lilian Edwards, 'Data Protection: Enter the General Data Protection Regulation' in Edwards L (ed), *Law, Policy and the Internet* (Hart Publishing 2018) (forthcoming) 46.
100 GDPR art 20(1) (emphasis added).

personal data is portable; and, *second*, that the relevant data must identify (currently or potentially) the data subject.

As discussed, the concept of personal data is extremely broad and might encompass a vast array of information. Anonymized data (as long as the anonymization is indeed effective) does not fall within the concept of personal data and, therefore, is outside the RtDP's scope. On the other hand, pseudonymized data is encompassed, as the data subject is identifiable.[101]

Clearly excluded is personal data only concerning other data subjects. Frequently, however, controllers process data relating to multiple data subjects, where the data is intrinsically intertwined, such as in e-mails, telephone and bank records, and group pictures. In such cases, personal data of other data subjects cannot be detached without the data losing its value and purpose. For what value is an e-mail, if one does not know with whom the communication is with? Or a photo with family, friends or colleagues, where other individuals are cut out or blurred?

In line with Recital 68 GDPR,[102] WP29 recommends not taking a too restrictive approach. If the receiving controller's processing does not adversely affect the rights and freedoms of such other data subjects (Article 20(4) GDPR), transmitting controllers should port the data.[103] This would be the case, for example, with a portability request for the content of a webmail or bank account.[104] How exactly this should be assessed by the transmitting controller is unclear and will most likely have to be decided by case-law.

Additionally, the RtDP solely applies to personal data that was provided by the data subject.[105] This restricts the right considerably, as personal data concerning the data subject, but provided to the controller by a third party, is excluded.[106] It even runs against the RtDP's rationale to prevent lock-in effects. For instance, photos and videos depicting the individual,

101 GDPR art 11(2) – if the controller cannot identify the data subject, there is no obligation to comply with a portability request. However, the data subject may provide additional information in order to enable the controller to identify her, which might be necessary especially for pseudonymized data.

102 GDPR rec 68, 7th sentence reads as follows: 'where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation'.

103 WP242 (n 14) 9.

104 Ibid 11.

105 GDPR art 20(1).

106 Veil (n 46) 609.

but posted by another user (even if on the data subject's page/profile) will not be subject to portability. And since social networks are largely about user interaction, not having this data ported might render the RtDP less appealing.

Furthermore, the expression 'provided by' is one of the most contended aspects, which, depending on its interpretation, narrows or broadens the RtDP's scope significantly.[107] The issue lies on the personal data taxonomy based on data origin, which was first discussed in 2014 within the Organisation for Economic Co-operation and Development (OECD).[108]

According to such taxonomy, there are four different categories of personal data: (i) *provided data* – actively and knowingly disclosed by the individual (eg filing of forms and posting on social networks); (ii) *observed data* – observed from the individual and recorded by a third party (eg online cookies and sensors); (iii) *derived data* – new data generated based on other data from the individual (eg computational and notational data); and (iv) *inferred data* – data resulting from probability-based analytic processes (eg statistical and profiling data).[109]

That 'provided data' is within the RtDP's scope has not been questioned, mainly in view of the Commission's emphasis on social networks.[110] On the other hand, passively provided data under the category of observed data has been disputed, as 'providing' is an active act.[111]

A restrictive interpretation would result in the RtDP's inapplicability to data collected through online activity (such as search history, traffic and location data) and connected devices[112] (such as fitness trackers and smart wearables). This would defy the very objective of the RtDP to provide individuals with greater control over their own data in the data economy, and already render the provision outdated at its birth.

---

107 Paul De Hert and others, 'The right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' [2017] CLSR, 7; Graef, Husovec and Purtova (n 7) 9; Gianclaudio Malgieri, ''User-provided personal content' in the EU: digital currency between data protection and intellectual property' (2018) 32 (1) IRLCT 118, 130; Ursic (n 87) 14.

108 OECD, 'Summary of the OECD Privacy Expert Roundtable on 21 March 2014 - Protecting Privacy in a Data-driven Economy Taking Stock of Current Thinking' [2014] DSTI/ICCP/REG(2014)3, 5.

109 Ibid.

110 Drexl, 'BEUC Study' (n 43) 108; Janal (n 78) 3.

111 De Hert and others (n 107) 7; Malgieri (n 107) 130; Veil (n 46) 610.

112 Connected devices can be defined as any device that is connected to other things and persons through mobile communication and which generate data. Drexl, 'BEUC Study' (n 43) 28.

As argued by Drexl and Janal, where personal data is collected from connected devices, data subjects are actually actively and knowingly using the device.[113] Both further reason that the wording of Recital 60 GDPR also speaks in favour of a broader interpretation, as it seems to consider collected data as a way to provide personal data. Similarly, Article 15(g) GDPR also does not clearly distinguish provided and collected data.[114] To reach its full value, WP29 considers that the concept of 'provided by' encompasses both provided and observed data, but not derived and inferred data.[115]

Exclusion of derived and inferred data is perceived as a balancing exercise with the supplier's intellectual effort in creating these forms of data.[116] The restriction prevents competitors from accessing the results of the processing efforts conducted by the first controller or on its behalf. However, it does not enable data subjects to derive the full benefit of their data in the digital economy.[117]

As stated by the Commission, 'like technology, the way our personal data is used and shared in our society is changing all the time' and our 'challenge (…) is to establish a legislative framework that will stand the test of time'.[118] In the data economy, individuals also need portability of their data collected through use of a service or device. Hence, the concept of 'provided by' should be construed as including data actively and knowingly provided, as well as observed data. This, nevertheless, should not prevent the scope's expansion in the future to adapt to new technological challenges.[119]

113 Drexl, 'BEUC Study' (n 43) 108-9; Janal (n 78) 3.
114 De Hert and others (n 107) 7; Malgieri (n 107) 130. Article 15(g) GDPR mentions 'data (…) collected from the data subject'.
115 WP242 (n 14) 10. Also recommended by the EDPS, OJ C 301/1 (n 51) 8, fn 34.
116 Graef, Husovec and Purtova (n 7) 9-10; Voigt and von dem Bussche (n 93) 170-1.
117 Banda (n 28) 45-46; Drexl, 'BEUC Study' (n 43) 156.
118 COM(2010) 609 final (n 17) 18.
119 See Drexl, 'BEUC Study' (n 43) 156, arguing that the exclusion does not protect the interest of making full use of connected devices.

4. The Exception of Rights and Freedoms of Others

The RtDP is not an absolute right, as Article 20(4) GDPR sets forth that it 'shall not adversely affect the rights and freedoms of others'.[120] Which 'others' could be affected by the RtDP is just as little specified as the possible affected rights and freedoms.

The neutral term 'others' renders the provision open to natural and legal persons. It is unclear, however, if such others relate to both the data subject and the controller, or only to the former. Should the reference be to both, then the controller could not raise its own rights and freedoms as impediment to a portability request. In contrast, should it refer solely to the data subject, the possibility would stand.

While WP29 and most literature abide to the first option,[121] this issue will most probably still have to be clarified by case-law. In any event, it is recommendable taking a cautious approach to not provide controllers with an excessively extensive power, undermining the RtDP.[122] Hence, the provision should ideally not allow the controller to raise its own rights and freedoms.

With regard to 'rights and freedoms', when assessing a portability request, controllers must, as discussed, also consider data protection rights of other data subjects in case of multi-personal data. It is coherent with the fact that personal data protection, just as all fundamental rights and freedoms, is not an absolute right. As recognized under Recital 4 GDPR, 'it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.

Nevertheless, considering the broad wording, one may argue that rights of others also cover IPRs. Regarding the right of access, Recital 63 GDPR, determines that it 'should *not adversely affect* the rights or freedoms of oth-

120 Although Article 20(4) refers only to paragraph 1 (indirect portability), the provision was actually intended to also apply to paragraph 2 (direct portability). In the text in preparation for the Trialogue, both rights were within paragraph 2, as paragraph 1 had been omitted. After renumbering, however, the reference was not appropriately amended. Moreover, the final German version of the GDPR still refers to paragraph 2 and, so, German literature refers normally to such paragraph, while commentators form other Member States refer to paragraph 1. See Council Doc ST 15039 2015 INIT (15.12.2015) 110, art 18(2), (2a).

121 Banda (n 28) 49-50; Graef, Husovec and Purtova (n 7) 15; Veil (n 46) 615; WP242 (n 14) 12.

122 Drexl, 'BEUC Study' (n 43) 84-5.

ers, including trade secrets or *intellectual property*' (emphasis added). There is, however, no equivalent provision expressly referring to the RtDP.

Borrowing the wording of Recital 63, WP29 states that

> The *rights* and freedoms *of others* mentioned in Article 20(4) (…) can be understood as "*including* trade secrets or *intellectual property* (…)". Even though these rights should be considered before answering a data portability request, "*the result of those considerations should not be a refusal to provide all information to the data subject*".[123]

There is no explanation on the rationale of such interpretation, but it can be inferred from the RtDP's legislative history, which created a close relationship with the right of access.[124]

It is noteworthy that, notwithstanding such connection, WP29 concludes that it should not result in the controller's refusal to provide all of the individual's data. Consequently, controllers should consider each piece of information separately when assessing a portability request. Refusal to port should only encompass that data adversely affecting an IPR or trade secret of others, not all data.[125]

Finally, the expression 'adversely affect' causes further uncertainty. While some authors characterize it as a balancing clause, which has to be asserted based on the particularities of the case,[126] others understand that the 'RtDP enjoys a lower rank compared to rights and freedoms of others'.[127] According to Drexl, the first construction not only leads to legal uncertainty, but is also not supported by other GDPR language versions.[128]

---

123 WP242 (n 14) 12 (emphasis added).

124 Graef, Husovec and Purtova (n 7) 10.

125 In case of photos in social networks, where the controller can establish that the individual is not the copyright owner, nor has a license, refusal to port should only affect this particular photo, not all personal data.

126 De Hert and others (n 107) 6. Graef, Husovec and Purtova (n 7) 14 also seem to favour a balancing exercise, considering their proposed differentiation based on the subsequent use of ported data.

127 Scudiero (n 73) 126. Note, however, that Scudiero then argues that 'controllers are called to perform a balance', which seems to favour a balancing clause interpretation.

128 Drexl, 'BEUC Study' (n 43) 84, fn 339, indicates the German and French versions, which come closer to full respect of the rights and freedoms of others. As a further example, we can cite the Portuguese version, stating that the RtDP 'não prejudica os direitos e as liberdades de terceiros' (does not prejudice the rights and freedoms of third parties).

In view of this, case-law will certainly be asked to deal with the issue shortly.

Considering the above, there seems to be no reason to exclude IPRs up front from the provision's applicability.

D. Data Portability Beyond Personal Data?

Even though this research's focus lies specifically on the RtDP, it is notable that portability is an emerging and trending concept in the EU, which goes beyond personal data.[129] The Commission already acknowledged data as an essential resource within the data economy and that unjustified restrictions on free flow of data might even jeopardize the full development of the EU data economy.[130] Data portability would be a means to ensure better access to data that, in turn, helps maximizing the value of data for society.[131]

As observed by Drexl, there is no reason to restrict portability to personal data, as lock-in effects also occur in non-personal data scenarios.[132] Most importantly, it is not limited to business-to-consumer (B2C) relationships, but also arises in business-to-business (B2B) settings. The EU legislator seems to understand and support such approach,[133] as two Commission proposals currently under discussion provide for portability related provisions.

The first is under the proposal for a Digital Content Directive, which applies to B2C contracts for supply of digital content, where a price is paid by the consumer or the consumer actively provides a counter-performance other than in money in form of personal or other data.[134] If adopted,[135] it

129 Graef, Husovec and Purtova (n 7) 2; Janal (n 78) 1.
130 COM(2017) 9 final (n 2) 2-3.
131 Commission, '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' SWD(2017) 2 final, 47.
132 Josef Drexl, 'Designing Competitive Markets for Industrial Data - Between Propertisation and Access' (2017) 8 (4) JIPITEC 257 para 1, para 157.
133 SWD(2017) 2 final (n 131) 48.
134 COM(2015) 634 final (n 16) art 3(1).
135 The proposal has already been subject to comments and proposed amendments by the Council and the European Parliament. There seems to be a tendency to leave any portability regime for personal data under the scope of the GDPR, but also to end up excluding data portability for non-personal data from the final

will provide consumers with a right to indirect portability after contract termination by the consumer, enabling retrieval of all content provided by her and any other data she produced or generated through the digital content's use.[136]

The second is within the proposal for a Regulation on the Free Flow of Non-Personal Data, which applies to the storage or other processing of electronic non-personal data.[137] Although the Commission's initial idea was to introduce a right to port, it ended opting for a self-regulation for non-personal data.[138] Under the proposed provision, the Commission would encourage and facilitate the development of self-regulatory codes of conduct, to establish best practices on portability.

The above highlights the RtDP's importance, which might be used as a basis to develop other portability schemes in the data economy.[139] Moreover, the relationship between the different portability forms has to be considered under the Commission's proposals to have a coherent outcome.[140]

---

text. For a detailed discussion on the amendments and their potential impact, see Drexl, 'BEUC Study' (n 43) 123-6; Axel Metzger and others, 'Data-Related Aspects of the Digital Content Directive' (2018) 9 (1) JIPITEC 90, 103-5.

136 COM(2015) 634 final (n 16) art 13(2)(c) (for termination in case of non-conformity of the delivered content) and art 16(4)(b) (for termination of long-term contracts).

137 COM(2017) 495 final (n 16) art 2(1).

138 Ibid art 6(1).

139 Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public Consultation on Building the European Data Economy"' (2017) Max Planck Institute for Innovation & Competition Research Paper No. 17-08 <https://ssrn.com/abstract=2959924> accessed 8 April 2018, para 25.

140 Graef, Husovec and Purtova (n 7) 24; Janal (n 78) 11; Metzger and others (n 135) 103.