Data portability under the GDPR: A blueprint for access rights?

Ruth Janal

A. Introduction

I. From ownership to access

With the rise of industry 4.0 and the advent of Big Data, data markets and data value chains are still evolving. The discussion about an adequate legal framework for the data economy has shifted its focus from an exclusionary right to data (ownership/IP right)[1] to the question of access to data.[2]

Under the EU's General Data Protection Regulation (GDPR), the data subject is granted 'portability', i.e. a right to receive the personal data relating to her or him and to transmit this data to another controller.[3] This paper explores whether the portability right might serve as a model for access rights in the business context. Let me briefly note that the Directive on contracts for the supply of digital content and digital services contains a

1 Herbert Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem Recht des "Datenerzeugers"' (2015) Computer und Recht 137, 144–46; Louisa Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' (2016) Computer und Recht 288, 294–96; Andreas Wiebe, 'Protection of industrial data – a new property right for the digital economy?' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 877, 881–84.

2 Josef Drexl and others, 'Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate' (2016) Max Planck Institute for Innovation and Competition Research Paper No. 16–10 <https://ssrn.com/abstract=2833165> accessed 31 August 2020; Lothar Determann, 'Gegen Eigentumsrechte an Daten: Warum Gedanken und andere Informationen frei sind und es bleiben sollten' (2018) Zeitschrift für Datenschutz 503, Jürgen Kühling und Florian Sackmann, 'Irrweg "Dateneigentum" – Neue Großkonzepte als Hemmnis für die Nutzung und Kommerzialisierung von Daten' (2020) Zeitschrift für Datenschutz 24.

3 Art. 20 Regulation (EU) No. 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, [2016] OJ L119/1.

similar provision, which however is limited in scope.[4] I will therefore limit my remarks to Article 20 GDPR.[5]

II. Overview of Article 20 GDPR

Under Article 20 GDPR, data subjects have the right to receive personal data that they have provided to a controller in a structured, commonly used and machine-readable format. Furthermore, data subjects have the right to transmit their personal data to another controller without hindrance. The right to portability constitutes an outlier amongst GDPR data subject rights. While most of the GDPR's rules shield the data subject from unwanted data use by others, Article 20 GDPR acts as a sword (albeit a blunt one): It grants data subjects the right to use (ie transfer) their personal data.[6]

The legislative intent behind Article 20 GDPR is not entirely clear. Its obvious purpose is to empower the data subject. However, this empowerment seems to serve a larger goal, namely, to facilitate competition among data controllers by preventing lock-in effects.[7]

---

4 Art. 16(4) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] L136/1. This rule only applies to non-personal data in cases of termination of a consumer contract regarding digital content. Even cat videos, sometimes cited as an example of data within the scope of that rule, often relate to a particular, identifiable person. The scope of the rule is further minimised by the fact that contracts relating to smart gadgets are not within the ambit of the regulation; cf. Gerald Spindler und Karin Sein, 'Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen: Anwendungsbereich und grundsätzliche Ansätze' (2019) Zeitschrift für IT-Recht und Recht der Digitalisierung 415, 416.

5 For other data access regimes cf. Inge Graf, Martin Husovec and Jasper van den Boom, 'Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes' (2019) TILEC Discussion Paper No. DP 2019–005 <https://ssrn.com/abstract=3369509> accessed 31 August 2020.

6 According to Recital 68 GDPR, data portability strengthens the data subject's control over his or her own data; see also Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (5 April 2017) Working Paper 242, 4 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 31 August 2020; Michael M. Maisch, *Informationelle Selbstbestimmung in Netzwerken* (Duncker & Humblot 2015) 311.

7 European Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10 January 2017, SWD(2017) 2

The portability right under Article 20 GDPR applies to personal data 'provided' by the data subject to a controller. As a further qualification, the right to portability only arises where the processing is carried out by automated means and is based upon consent or contract (Article 6(1)(a), (b); Article 9(1)(a) GDPR). The controller must transmit this data to the data subject in a structured, commonly used and machine-readable format, acting without undue delay and generally within one month at the latest (Article 12(3) GDPR). Where technically feasible, the data subject may require the controller to transfer the data directly to another controller. Portability can be required at any point in time and is in principle free of charge.[8] The right to receive the data is subject to three exceptions: First, a transmission of data cannot be requested with respect to data that has already been deleted or anonymised.[9] Second, the portability right may not interfere with a task carried out in the public interest.[10] Third, portability shall not adversely affect the rights and freedoms of others.[11]

---

final, 11. Niko Härting, 'Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf' (2012) Betriebs-Berater 459, 465; Dennis-K. Kipker and Friederike Voskamp, 'Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung (2012) Datenschutz und Datensicherheit 737, 740; Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?' (2016) Europäische Zeitschrift für Wirtschaftsrecht 448, 450; Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht' (2016) Neue Juristische Wochenschrift 1841, 1845; Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359, 1365; Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' (2019) Gewerblicher Rechtsschutz und Urheberrecht 569, 574; Alexander Dix, in Alexander Dix, Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), Datenschutzrecht (4th edn, Nomos 2019) Art. 20 DSGVO para. 1; Deutsche Bundesregierung (Federal Government of Germany), 'Antwort der Bundesregierung auf die Kleine Anfrage' (Deutscher Bundestag 10 August 2012) Bundestags-Drucksache 17/10452, 7 <dipbt.bundestag.de/doc/btd/17/104/1710452.pdf> accessed 31 August 2020. For the economic consequences of portability cf. European Commission SWD (ibid) 47 et seq.

8 Art. 12(5) GDPR. This does not apply to manifestly unfounded or excessive (i.e. repetitive) requests. Article 29 Data Protection Working Party (n. 6) 12 argues that '[f]or information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden'.

9 Art. 20(3), sentence 1 and Recital 26 GDPR; Article 29 Data Protection Working Party (n. 6) 7.

10 Art. 20(3) sent. 2. On the concept of public interest cf. Recital 73 GDPR.

11 Art. 20(4) GDPR.

III. Structure of Arguments

Any attempt to draw inferences from Article 20 GDPR about the business world must first query the similarities of the two settings. In the following, I will first expound on how a B2B setting differs from the data context of the GDPR. In the light of this analysis, the paper then focuses on several key ambiguities of Article 20 GDPR and how these issues might translate to the business scenario: (1) The data covered by the right to portability, (2) the protection of the rights and freedoms of others and (3) the modus operandi of 'portability'.

B. Distinctions between the GDPR setting and a B2B scenario

When considering whether Article 20 GDPR can function as a blueprint for a business portability right, one needs to keep in mind that a B2B scenario often differs significantly from the scenario regulated by the GDPR. In the following, I will highlight some of the key differences.

I. Personal data and non-personal data

While the GDPR only pertains to personal data, the interest of the business world is not limited to such data. Commercial value may lie in all kinds of data, personal and non-personal data alike.

II. Attribution of data

1. The GDPR setting

More importantly, the GDPR provides for a clear attribution of data. The Regulation addresses personal data concerning an identified or identifiable individual and bestows rights upon data subjects because the data processed relates to their personal identity. If the data relates to several identifiable individuals (such as pictures, chat records and data generated by shared gadgets), the data is attributed to each of these individuals. Admittedly, the regulation does not provide for a clear mechanism on how to resolve a conflict of interest between data subjects. This may be due to the

fact that such multi-polar personal data is hardly the norm (the exception being data processed by social networks).

2. The business setting

a) Lack of legal attribution

With respect to business data, such a clear legal attribution of data to any one party cannot be identified.[12] In practice, the data is either attributed on the basis of factual barriers to access or on the basis of data-sharing agreements.[13] However, there is no common ground as to which connecting factors are sufficient to deem data as legally related to a particular business. Nor is there generally a right to confidentiality or even a reasonable expectation of confidentiality with respect to data. Furthermore, using Article 4(1) GDPR (the criterion of identifiability) as a model for attribution will not work. In the business context, the possibility of identification is not an adequate criterion for attribution. Data relating to an identifiable natural person is protected because the identity is a core element of a human's existence. In a business context, data is not an element of identity, but rather allows for value creation.[14] Since data is a tradeable commercial commodity,[15] and businesses may purchase data from others, identifiability should not even be used as a minimum criterion.

12 Martin Fries and Marc Scheufen, 'Märkte für Maschinendaten: Eine rechtliche und rechtsökonomische Standortbestimmung' (2019) Zeitschrift für IT-Recht und Recht der Digitalisierung 721, 721; Udo Kornmeier and Anne Baranowski, 'Das Eigentum an Daten – Zugang statt Zuordnung' (2019) Betriebs-Berater 1219, 1223; Specht (n. 1) 289.

13 Kornmeier and Baranowksi (n. 12) 1221.

14 Fries and Scheufen (n. 11) 721; Schweitzer (n. 7) 569–70.

15 Jutta Stender-Vorwachs and Hans Steege, 'Wem gehören unsere Daten? Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs' (2018) Neue Juristische Online-Zeitschrift 1361; Herbert Zech, 'Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt' (2015) Gewerblicher Rechtsschutz und Urheberrecht 1151, 1151–52.

b) Multi-relational nature of data

Business data is also typically multi-relational. Personal data which is processed for business purposes will relate to the business' customers or employees as well as the business itself. Furthermore, in interdependent manufacturing chains or service industries, data often relates to the interests of various market players.[16] Consider an enterprise resource planning (ERP) system employed for quality control in industrial production: A machine which manufactures metal sheets is equipped with a camera that examines the sheets for manufacturing defects and determines rejections. The data regarding rejections is finally analysed using applications running on a cloud infrastructure. This data will relate to various businesses: the supplier of both the raw material and the machines, the manufacturer as well as the data processor. Should the data be attributed to all these businesses or is one business 'more worthy' than the other? In its communication 'Towards a common European data space', the European Commission expresses the hope that contracts 'recognise that, where data is generated as a by-product of using a product or service, several parties have contributed to creating the data.'[17] The Commission does not substantiate what kind of contribution it deems significant enough for a business to have contributed to such shared value creation.

c) The Trade Secrets Directive

Arguably, some legal attribution of data is achieved by means of the Trade Secrets Directive,[18] even though the Directive does not create any exclusive

16 Wolfgang Kerber, 'Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Hart and Nomos 2017) 109, 127–28; also Herbert Zech, 'Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt' (2015) Gewerblicher Rechtsschutz und Urheberrecht 1151, 1156.

17 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 'Towards a common European data space' COM(2018) 232 final.

18 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1. Legal attribution of data as a consequence of the Directive is discussed by Lukas Staffler, 'Industrie 4.0 und wirtschaftlicher Geheimnisschutz' (2018) Neue

right to know-how or information.[19] Rather, the Directive shields the trade secret holder against unlawful acquisition, use and disclosure of trade secrets (i.e. information that is secret, is of commercial value because it is secret and has been subject to reasonable steps to be kept secret). It is noteworthy that a trade secret holder is defined by the Directive as a person lawfully controlling a trade secret. Whatever the meaning of 'lawful control',[20] any such person would presumably not have to rely on a portability right for a transfer of data, because they would already possess the necessary control.

III. Structural power imbalances

Under the GDPR, the relationship between the data subject and the data controller is characterised by a structural power imbalance. Typically, the data controller is a business or public body, whereas the data subjects are consumers who often have little choice in how their data is processed.

Business scenarios are much more diverse. For example, a machine builder who also processes industrial data may or may not be in a more powerful economic and negotiating position than its customer: The machine builder might be a small start-up that provides autonomous mobile robots to an international logistics company. The machine builder could just a well be a major automaker selling cars to a small courier service. Alternatively, the parties' bargaining position could be equal. In the absence of clear structural power imbalances, an argument may be made that a contractual right to portability should be left to the parties' negotiation

---

Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 269, 273; Andreas Wiebe, 'Protection of industrial data – a new property right for the digital economy?' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 877, 881–84; Zech (n. 16) 1155–56.

19 Recital 16 Directive (EU) 2016/943.

20 For the discussion of whether 'control' is to be determined purely on a factual or also on a normative basis cf. Staffler (n. 18) 272 et seq. (arguing for the introduction of normative criteria). Arguing for a determination simply upon factual criteria; Michael Goldhammer, 'Geschäftsgeheimnis-Richtlinie und Informationsfreiheit: Zur Neudefinition des Geschäftsgeheimnisses als Chance für das öffentliche Recht' (2017) Neue Zeitschrift für Verwaltungsrecht 1809, 1810 et seq.; Björn Kalbfus, 'Die EU-Geschäftsgeheimnis-Richtlinie: Welcher Umsetzungsbedarf besteht in Deutschland?' (2016) Gewerblicher Rechtsschutz und Urheberrecht 1009, 1011.

and legislation should only concern itself with portability obligations imposed upon dominant undertakings.

IV. Remuneration for data analysis

The saying 'You are not the customer, you are the product' illustrates a third major difference between data subjects and businesses seeking portability: Individual data subjects usually do not pay the data controller for an analysis of their data.[21] Rather, data controllers process and analyse the customer data in their own interest, which is sometimes so profitable that they need not charge their customers for the services offered. Again, this may be very different in a B2B context. For example, the Airbus Skywise platform allows participating airlines to deeply analyse the airline fleet's reliability and the passengers' behaviour – for a fee, of course.

V. Commercial value

Finally, an individual's personal data is typically of little commercial value.[22] Commercial benefits from the processing of personal data typically arise from the pooling of data across a large customer base. Consequently, there is relatively little outside interest in the transfer of one particular individual's data. In contrast, the data sets generated by an individual company or individual segments of their business are oftentimes already large enough to generate both internal as well as outside interest.

VI. Summary

In sum, a portability B2B scenario differs immensely from the scenario addressed by Article 20 GDPR: The data requested may include both personal and non-personal data. The data is not legally attributed to the business making the portability request. A typical structural power imbalance between the party making the request and the addressee of the request can-

21 This may be different with respect to some smart gadgets, such as fitness trackers.

22 Marcel Bisges, 'Personendaten, Wertzuordnung und Ökonomie: Kein Vergütungsanspruch Betroffener für die Nutzung von Personendaten' (2017) Zeitschrift für IT-Recht und Recht der Digitalisierung 301, 302.

not be identified. The controller may have been remunerated for data analytics services, and the commercial value of the data requested may be much higher than in cases of requests under Article 20 GDPR.

C. Transfer of ideas and principles

Keeping those key differences in mind, let us now return to Article 20 GDPR. In the following section, I shall explore whether Article 20 GDPR leads itself to generalisations. In doing so, I will focus on three critical aspects of the provision which are ambiguous: (I) Which data is covered by the right to portability, (II) how can the rights and freedoms of others be protected and (III) what is the adequate modus operandi of 'portability'?

I. The data encompassed

1. Data covered by Article 20 GDPR

Under Article 20(1) GDPR, the data subject shall have the right to receive and transmit data 'which he or she has provided to a controller', where the legal basis for processing is consent or contract. Clearly, the wording of the provision covers personal data explicitly provided by the data subject, such as contact information, comments und uploaded material. It is also undisputed that information which the data controller has inferred from its customers' data does not constitute data 'provided' by the data subject. As a result, data derived by means of aggregation and analysis, such as user profiles and credit scores, are not subject to the portability requirement of Article 20 GDPR.[23]

Other personal data falls between these poles. This is true for data which a third party has provided to the controller based on a relationship with the data subject, in particular all communication sent to the data subject (emails, chat records, comments on posts etc.). The wording of Article 20 GDPR does not seem to encompass such data.[24] On the other hand, the

23 Article 29 Data Protection Working Party (n. 6) 10; Stiftung Datenschutz, 'Practical Implementation of the Right to Data Portability – Summary and Recommendations' (2017) 7 <www.stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/kurzversion_studie_datenportabilitaet.pdf> accessed 31 August 2020.

24 Some authors even argue that any data with a third-party relation is not covered by Art. 20 GDPR; cf. Tim Jülicher, Charlotte Röttgen and Max v. Schönfeld, 'Das

ability to transfer this data is important for data subject empowerment and the prevention of lock-in effects. The Article 29 Data Protection Working Party (the predecessor of the European Data Protection Board), considers such data to be covered by Article 20 GDPR (without offering any explanation).[25]

There is also a vigorous debate as to whether Article 20(1) GDPR covers data that the data controller has observed from the data subject's behaviour, specifically data regarding the use of a smart gadget or the use of a digital service. Arguably, such data is 'collected' by the controller, rather than being 'provided' by the data subject.[26] But it is important to stress that Article 20(1) presupposes a lawfulness of processing based upon consent or contract. Consequently, the data subject has willingly allowed the controller to collect this data and thus provided access to it.[27] This broader interpretation is supported by Article 60 sent. 4 GDPR which considers collection as a form of provision of data ('Where the personal data are collected from the data subject, the data subject should also be informed

---

Recht auf Datenübertragbarkeit: Ein datenschutzrechtliches Novum' (2016) Zeitschrift für Datenschutz 358, 361.

25 Article 29 Data Protection Working Party (n. 6) 11; see also Schantz (n. 7) 1845.

26 Carlo Piltz, in Peter Gola, Datenschutz-Grundverordnung DS-GVO, Kommentar (2nd edn, C.H. Beck 2018) Art. 20 para. 14–15; Sebastian Brüggemann, 'Das Recht auf Datenportabilität' in Jürgen Taeger (ed.), *Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren* (Oldenburger Verlag für Wirtschaft, Informatik und Recht 2017) 1, 4; Hans-Georg Kamann and Martin Braun, in Eugen Ehmann und Martin Selmayr (eds), Datenschutz-Grundverordnung: DS-GVO, Kommentar (2nd edn, C.H. Beck 2018) Art. 20 para. 13; Handelsverband Deutschland e.V., 'Antworten des Handelsverbands Deutschland auf die Fragestellungen hinsichtlich des RL-Entwurfs für Verträge über digitale Inhalte' (2016) 2 <www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/AbteilungenReferate/IB6_VA_Digitales_Vertragsrecht_Stellungnahme_HDE_2.pdf?__blob=publicationFile&v=1> accessed 31 August 2020.

27 Article 29 Data Protection Working Party (n. 6) 10: Observed data are 'provided' by the data subject by virtue of the use of the service or the device. The European Commission SWD (n. 7) 46, seems to share this view. See also Lukas Dalby, in Gerald Spindler and Fabian Schuster (eds), *Recht der elektronischen Medien* (4th edn, C.H. Beck 2019) Art. 20 DS-GVO para. 7–8; Moritz Hennemann, 'Datenportabilität' (2017) Privacy in Germany 5, 6–7.; Peter Krause 'Datenportabilität: Anwendungsbereich des Rechts auf Datenübertragbarkeit (Teil 1)' (2018) Privacy in Germany 239, 240–42; Maisch (n. 6) 304; Gerald Spindler, 'Verträge über digitale Inhalte – Haftung, Gewährleistung und Portabilität: Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte' (2019) Zeitschrift für IT-Recht und Recht der Digitalisierung 219, 222.

whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data').

Data should thus be considered as 'provided' by the data subject whenever the data subject willingly contributed to the acquisition of such data and the controller did not add any value to the data besides storage. This would encompass both communication to the data subject provided by third parties and observed personal data. Let me point out that much of the data collected on the data subject's behaviour will be helpful neither in empowering the data subject nor in preventing lock-in effects. Consider, for example, the amount of data collected by online shops or online streaming services on individual customers, which includes the entire clickstream up to buying an article or watching a movie, times of purchase and devices used, abandoned searches and so forth.[28] As I have argued elsewhere, it seems prudent to make the right to data portability subject to a proportionality requirement.[29]

2. *Data that might be covered by a business portability right*

While the interpretation of Article 20 GDRP is ambiguous, drawing inferences for a B2B scenario is even more complicated.

a) Beneficiary and addressee

Any new right would need to define a beneficiary and an addressee. The GDPR bestows a right to receive the data on data subjects. But as I have explained above (section B.I.), it is not clear who the beneficiary of a busi-

28 Katharina Nocun, 'Netflix weiß, was ich letzten Sommer geguckt habe' (21 August 2018) Die Zeit <www.zeit.de/digital/datenschutz/2018-08/streaming-dienst-netflix-datenschutz-nocun> accessed 31 August 2020.

29 Ruth Janal, 'Data Portability – A Tale of Two Concepts'(2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 58, 62; cf. Christoph Werkmeister and Elena Brandt, 'Datenschutzrechtliche Herausforderungen für Big Data' (2016) Computer und Recht 233, 237; Stiftung Datenschutz (n. 23) 3; Sebastian Brüggemann, 'Das Recht auf Datenportabilität: Die neue Macht des Datensubjekts und worauf Unternehmen sich einstellen müssen' (2018) Kommunikation & Recht 1, 4. Note also Art. 16(4) Directive (EU) 2019/770 on digital content and digital services (n. 4).

ness portability right should be, as a legal attribution of such data is missing.

The addressees of a new portability right would also have to be defined. Portability under Article 20(1) GDPR may be requested from the controller, ie any person who, 'alone or jointly with others, determines the purposes and means of the processing of personal data' (Article 4 No. 7 GDPR). This definition would not serve well in a business context, as it is equally too broad and too narrow. In a business setting, the business requesting portability might be the person who determines the purposes of the processing, whereas the person from whom the data is requested might only be a 'processor' within the meaning of Article 28 GDPR.

Further, in cases of joint control, Article 26(3) GDPR allows data subjects to exercise their rights against any of several joint controllers. Suppose a business regularly uses a specific airline for company travel and now realises that this airline uses the Airbus Skyways Platform. Suppose that same business delivers components to a manufacturer which has a data-sharing agreement with a machine builder. If the GDPR's model was copied, this business would be allowed to request data from anyone along the contractual chain, as long as the addressee could be considered a 'joint controller'.

b) Data provided because of a contract or consent

In the absence of a clear attribution of business data to an individual business (above at section B.I.), the beneficiary of a business portability right needs to be determined based upon other criteria. These criteria must be set to fit the purpose of the rule. If the prime purpose of an eventual portability right was to minimise data lock-in, the portability right could be made contingent upon the existence of a contractual relationship between the business making the request and the addressee. However, there is also discussion of introducing a business portability right to facilitate data-driven aftermarket and complementary services and enhance competition. This purpose would not be served if the existence of a contract was made a requirement for portability, as contractual relations between competitors are not the norm.[30]

Article 20 GDPR allows for a portability request only if the data is being processed because of consent or based on a contract. Since the processing of non-personal data does not require consent, relying on consent for a

30 Cf. Schweitzer (n. 7) 575.

portability right to arise might lead to random results. While some industry players may ask their suppliers and co-operating businesses to consent to the processing undertaken by a commissioned controller, others may not. Arguably, therefore, the existence of a contractual agreement is a better criterion in the business context. But should any kind of contract suffice? Or is a distinction warranted between data-sharing agreements, contracts pertaining to digital services, confidentiality agreements (required to safeguard trade secrets in accordance with Article 2(1)(c) Trade Secrets Directive) and classic sales contracts? One option might be to exclude contracts which do not entail a digital transfer of data. With this distinction, a portability right would arise (a) from contracts for digital content and services and (b) from sales and rental contracts for IoT machinery and connected means of transportation. A portability right would not arise from sales contracts regarding unconnected goods.

c) Observed and inferred data

Unlike an individual data subject, a business user will ordinarily be very interested in the 'observed' data generated by their company's use of machines or digital services. A private data subject will generally not be able to reuse observed data in a different context. From a business perspective, however, there is tremendous value in observed data.[31] A portability right encompassing observed data will put the business in the position to sell or further process such data. Also, retention of data that was originally provided by others, such as employees and suppliers, may be of vital interest to the business. If a portability right for businesses is to be introduced, it should encompass any data that was originally willingly transferred from the business' sphere to the controller, irrespective of whether the data was actively supplied by the business, collected from machines or supplied by others on the basis of a relationship with the business. Insofar, a parallel may be drawn to the interpretation of Article 20 GDPR suggested above.

There is, however, an important distinction to be drawn between the portability right under Article 20 GDPR and a possible business portability right: In the B2B context, a data controller will often be compensated by businesses for the retention and analysis of their data (fleet analysis, predictive maintenance, heating cost accounting and so forth). If a business has provided remuneration for the creation of 'inferred data', such data should

31 Ibid. 569.

be within the scope of any data portability right. In other instances, data analytics services are provided on a seemingly gratuitous basis. Such 'gratuitous services' may be a calculated choice in the interest of customer retention[32] and may not generate any additional cost for the service provider if the data is analysed anyway. Particularly in the case of predictive maintenance, such services will often be cross-financed through the purchase price or rental cost of the machines sold or rented. Thus, there is a strong case to be made that the portability right should apply to 'inferred data', even if such a service was offered on a seemingly gratuitous basis.

d) Preliminary findings

In short, there is considerable debate about the scope of data within the realm of Article 20(1) GDPR, and no definite inferences can or should be drawn with respect to the scope of a potential data portability right for businesses.[33] Rather, Article 20(1) GDPR demonstrates that any future legislature needs to carefully consider what kind of data is to be subject to an eventual portability right. Moreover, clear wording is needed to cast such intentions in law.

II. Rights and freedoms of others

1. Relevant rights and freedoms of others under the GDPR

Following Article 20(4) GDPR, the right to data portability 'shall not adversely affect the rights and freedoms of others'. This is a rather vague spec-

32 Esther Bollhöfer, Daniela Buschak, Christian Lerch and Matthias Gotsch, 'B2B-Dienstleistungen im Kontext von Industrie 4.0 – Neue Formen der Interaktion im Maschinen- und Anlagenbau' in Manfred Bruhn and Karsten Hadwich (eds), *Interaktive Wertschöpfung durch Dienstleistungen – Strategische Ausrichtung von Kundeninteraktionen, Geschäftsmodellen und sozialen Netzwerken* (Springer 2015) 517, 521; cf. Christian van Husen, 'Neue Serviceprodukte in industriellen Wertschöpfungsnetzwerken' in Bruhn and Hadwich (ibid.) 493, 503; Björn Ivens, Stephan Henneberg and Sebastian Forkmann, 'Service Infusion im Industriegütermarketing – Konzept, Wertschöpfung, Wirklichkeit' in Manfred Bruhn and Karsten Hadwich (eds), *Service Value als Werttreiber – Konzepte, Messung und Steuerung* (Springer 2014) 267, 279.

33 Datenethikkommission, 'Gutachten der Datenethikkommission der Bundesregierung' (2019) 137.

ification, to say the least. Let us start with the easy part: What are the rights and freedoms that might stand in the way of portability? The provision seems to mainly address personal data of other data subjects and trade secrets of the data controller and/or other parties.[34] Economic interests of the controller are not to be considered: First, Article 12(5) GDPR provides that the portability request must generally be fulfilled free of charge. Secondly, the entire purpose of Article 20 GDPR is to enable the data subject to change service providers and/or engage in multi-homing, which both may lead to adverse economic effects for the controller.

2. *Balancing of interests under the GDPR*

a) Data rights of third parties

The transfer of data either to the data subject or to another controller under Article 20(1) and (2) GDPR constitutes a processing of data within the meaning of Article 4 No. 2 GDPR. Insofar as the data is only related to the data subject making the request, this processing is covered by consent under Article 6(1)(a) GDPR. However, a picture may show more than one person and communication by its very meaning requires a minimum of two parties communicating. Insofar as the data also relates to other data subjects, the transfer of data must either be covered by their consent or be covered by another lawful basis for transmission.[35]

If the other data subject does not provide consent or cannot be reached for consent, Article 6(1)(f) GDPR may provide a legal basis for the transfer of data.[36] Under this provision, the processing is lawful if it is necessary for the purposes of legitimate interests of third parties (i.e., the data subject requesting portability), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Consequently, the portability of data relating to more than one data subject requires either consent of all the data subjects concerned or depends upon a balancing of interests of the respective individuals' data rights. The balanc-

34 Cf. Recital 63. sentence 5, regarding the right of access (Art. 15 GDPR). See also Kai von Lewinski, in *Beck Online-Kommentar Datenschutz-Grundverordnung* (31st edn, C.H. Beck 2020) Art. 20 para. 99; Judith Klink-Straub and Tobias Straub, 'Vernetzte Fahrzeuge – portable Daten: Das Recht auf Datenübertragbarkeit gem. Article 20 DS-GVO' (2018) Zeitschrift für Datenschutz 459, 462.

35 Piltz (n. 26) Art. 20 para. 23.

36 Article 29 Data Protection Working Party (n. 6) 11.

ing of interests will lead to different results depending on who supplied the respective data and under which expectations such data was provided. If the data was originally supplied by the individual who requests the transmission, the data rights of other parties do not stand in the way, as long as the new controller processes the data for the same purposes as the original controller.[37] Thus, a user who has provided a service provider with a list of their contacts can request a transfer of this contact information to another controller, even though the list includes the personal data of third parties.

As I have argued above, the data 'provided' by the data subject within the meaning of Article 20(1) GDPR may also in fact be supplied by other individuals (i.e. in case of emails and other communication) or may be collected from a gadget or service shared by several data subjects. Where the data was provided by a third party, the transfer request should not be fulfilled if there was a reasonable expectation on the part of the other data subject that the processing of information would be confined to a particular controller.[38] A person who sends an email or sends a credit transfer will generally not expect the addressee to keep the receiving account until the end of time, nor will they care if the addressee switches providers. On the other hand, a person who sends a communication within a closed social media group may very well have a reasonable expectation that this data will only be processed by the particular social networking provider. This is even more true in instances where the data was generated by a shared gadget, as the transfer to another controller may imply a change of gadget and thus possibly a change of users. In those instances, the right to portability will have to be denied, absent the consent of the other data subject.[39]

b) Trade secrets

There is some discussion that a transmission of data under Article 20 GDPR might also be thwarted if it led to the disclosure of the controller's trade secrets. Arguably, the 'rights and freedoms of others' referred to in

37 Von Lewinski (n. 34) Art. 20 para. 97; sceptical Jülicher and others (n. 24) 361–362.
38 Janal (n. 29) 62.
39 Klink-Straub and Straub (n. 34) 462.

Article 20(4) GDPR also include the rights and freedoms of the controller.[40] As Article 4 Trade Secrets Directive only protects the trade secret holder against unlawful acquisition, use and disclosure of a trade secret, the request for portability does not fall within the ambit of the Trade Secrets Directive.[41] Nonetheless, the interest of the controller to protect an existing trade secret may be considered under Article 20(4) GDPR. Such secrets might include the amount of data processed, the structure of the data processed and possibly accompanying metadata. It is hard to see how the interest in keeping this information secret could outweigh the data subject's right to portability. The GDPR certainly does not recognise a controller's right to keep secret the amount of personal data processed; Article 15 GDPR rather provides for the exact opposite. Also, considering the scope for implementation that Article 20 GDPR grants to the controller, it is incumbent upon the controller to organise the transmission in a way that does not reveal structural and metadata information.

3. Duty of care when complying with a portability request

Article 20 GDPR does not spell out the degree of care borne by the controller in complying with a portability request. The controller must certainly guarantee that the person requesting portability is the person who has either formed the contract or given the consent that is a prerequisite for the portability right to arise under Article 20(1)(a) or (b) GDPR.[42] Empirical studies show that a lot is left to be desired with respect to such verification procedures.[43] In case the data relates not only to the person making the request, but also to other individuals who have allegedly consented

---

40 While Recital 68, sentence 6, only refers to third parties when expounding on Art. 20(4) GDPR, Recital 63, sentence 5, clarifies regarding the similarly worded Art. 15(4) GDPR that interests of the controller may be taken into account. Cf. also Piltz (n. 26) Art. 20, para. 36; of a differing opinion Matthias Rudolph, in Rolf Schwartmann, Andreas Jaspers and Gregor Thüsing (eds), *Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, Kommentar* (C.F. Müller 2018) Art. 20 para. 109.

41 Apparently of a different view von Lewinski (n. 34) Art. 20 paras 101 et seq.

42 Recital 64: 'The controller should use all reasonable measures to verify the identity of a data subject' making the request; see also Stiftung Datenschutz (n. 23) 4.

43 Dominik Herrmann and Jens Lindemann, 'Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights?' in Michael Meier, Delphine Reinhardt and Steffen Wendzel (eds), *Sicherheit 2016 – Sicherheit, Schutz und Zuverlässigkeit* (Gesellschaft für Informatik e.V. 2016) 149.

to the transfer, the identity of those other data subjects must also be verified. The scope of such duties is – as of yet – undefined. I.e., it is unclear whether the controller is obliged to investigate whether an IoT gadget is used by several parties, which might exclude the right to portability.

Finally, some argue that in instances of direct transmission to a new controller, the old controller should provide the data subject with information regarding the usage envisioned by the new controller.[44] In my view, such an obligation should not be imposed: The new controller is also bound by the GDPR's rules, and it is a) upon the data subject to safeguard their rights vis-à-vis a new controller and b) upon the new controller to inform the data subject about its processing intentions in accordance with Article 13 GDPR.

4. Inferences for a business portability right

With respect to a possible portability right for businesses, it is possible to identify three groups whose interests may interfere with the portability request: Individuals whose personal data is contained amongst the data sets, third-party businesses with secrecy interests regarding the data sets and the economic interests of the service provider who is asked to transfer the data.

With respect to personal data (ie of customers and employees), the migration of data from one service provider to another constitutes a processing of data under Article 4 No. 2 GDPR and must be covered by a lawful basis in accordance with Article 6 GDPR. The transfer of data will generally not pose a problem if the person requesting the transfer is considered a controller for the purposes of the GDPR and the addressee of the request is a processor (Article 28 GDPR). However, if the parties possess joint control (Article 26 GDPR), the migration of personal data might currently lack a basis in law. The introduction of a portability right for businesses would impose a legal obligation to process data and could thus provide a lawful basis under Article 6(1)(c) GDPR. However, I suggest that the GDPR should generally take precedence over a business portability right and that any such right should clarify that the migration of personal data is subject to the restrictions of the GDPR.

---

44 Article 29 Data Protection Working Party (n. 6) 19; Personal Data Protection Commission of Singapore, 'Discussion Paper on Data Portability' (25 February 2019) 19–20 <www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf> accessed 31 August 2020.

The data stored may not only contain information regarding third-party data subjects, but also information regarding third-party businesses. In the absence of the legal attribution of data to a specific business (section B.II. above), the law does not require third parties to consent to the transfer of non-personal data. Trade secrets are an exception: Secret information of commercial value which has been subject to reasonable steps to be kept secret may not be divulged to non-authorised parties by any other party than the trade secret holder (Article 4 Trade Secrets Directive). In the case of digital storage of information, data can only be considered a trade secret if the parties involved have formed a confidentiality agreement. Thus, the addressee of any portability request may refuse the transfer of data, unless each trade secret holder has released them from the confidentiality agreement.

Finally, the interests of the addressee of the portability request need to be considered. However, I suggest that the adequate balance of interests between the party requesting portability and the addressee is achieved by defining the scope of the portability right, not through the insertion of an exception à la Article 20(4) GDPR. As has been explained above (section C.I.2.), the adequate balance between the interests of the parties depends upon the legislative objective of any future business portability right: A portability rule to enhance competitive markets should provide less access to data than a rule granting portability after the termination of a remunerated data analytics contract.

III. Modus operandi

1. The implications of portability under the GDPR

Under Article 20 GDPR, the data subject 'shall have the right to receive the personal data […] in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller'. Figuratively speaking, portability of data is envisioned like a jacket returned from a theatre's cloakroom: All data is handed over either to the data subject or to another controller once the data subject issues their request. This 'download your data' concept is exemplified by Google Takeout – a feature allowing google users to download their user archive.[45] Of course, unlike the jacket in the cloakroom after a return request, the data

45 <http://takeout.google.com/settings/takeout> accessed 31 August 2020.

on the controller's servers will remain there after a portability request, unless the data subject also requests the deletion of data.

In practice, data is probably more often than not transferred to another controller on the basis of co-operation agreements. An app or web service will allow the user to 'sign in with' their Google, Facebook, Microsoft or Apple account. The amount of data which is thereupon shared via the API varies from provider to provider.[46] In my view, such a model does not constitute 'portability' in the meaning of Article 20 GDPR. Rather, the transfer of data in those instances is a case of mutual processing under Article 26 GDPR. Initiatives such as the Data Transfer Project[47] aim to 'allow individuals to transfer their data seamlessly between online service providers'[48] using a platform-model. However, the co-operation of major players such as Google, Facebook, Apple, Microsoft and Twitter may lead to an even greater distribution of personal data and must therefore be observed closely. The platform-model portability envisaged by major data controllers may not necessarily be the scheme that is data protection-friendly. When Mark Zuckerberg announces that '[t]rue data portability should look more like the way people use our platform to sign into an app than the existing ways you can download an archive of your information',[49] this brings back not-so-pleasant memories of the Cambridge Analytica scandal.[50]

---

46 Antonie Moser-Knierim, '"Facebook-Login" – datenschutzkonformer Einsatz möglich? Einsatz von Social Plug-ins bei Authentifizierungsdiensten' (2013) Zeitschrift für Datenschutz 263; Amanda Schupak, 'What are you sharing when you sign in with Facebook or Google?' (3 November 2015) CBS News <www.cbsnews.com/news/what-are-you-sharing-when-you-sign-in-with-facebook-or-google/> accessed 31 August 2020.

47 <https://datatransferproject.dev> accessed 31 August 2020.

48 For Facebook see its White Paper: Erin Egan, 'Data Portability and Privacy – Charting a Way Forward' (6 September 2019) <https://fbnewsroomus.files.wordpress.com/2019/09/data-portability-privacy-white paper.pdf> accessed 31 August 2020.

49 Marc Zuckerberg, 'The Internet Needs New Rules. Let's Start in These Four Areas' (30 March 2019) Washington Post <www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html> accessed 31 August 2020.

50 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (17 March 2018) The Guardian <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 31 August 2020.

It is important to note that Article 20 GDPR does not provide for real-time portability.[51] In principle, the rule envisions a single-time transfer of data. Multiple requests within a reasonably long timeframe will also succeed. If the requests become repetitive, however, they may be deemed excessive and be refused or made subject to a fee under Article 12(5) GDPR. Thus, the right basically guarantees an option to change service providers.[52] It may also facilitate the beginning of multi-homing, but does not allow for a constant cross-use of different services.

2. *Data format*

Data is to be transferred in a 'structured, commonly used and machine-readable format' (Article 20(1) GDPR). The Regulation does not offer any guidance for situations in which a commonly used format does not exist. Further, a direct transmission from one controller to another can be required 'where technically feasible' (Article 20(2) GDPR). The latter requirement is quite curious: It is hard to think of an example where transmission to the data subject is feasible, but transmission to another controller is not. Thus, Article 20(2) seems to address inter-operability. This interpretation is supported by Recital 68: While 'data controllers should be encouraged to develop interoperable formats', the portability right 'should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.' The implication is that the right to portability fails in the absence of commonly used data formats.[53] Adding to the lack of clarity, there is no indication whether 'feasibility' is to be determined on the basis of objective standards or subjective criteria tailored to the person of the controller.[54] A suggestion by the Council of

51 Cf. the time period upon which to act under Art. 12(3) GDPR; see also Schweitzer (n. 7) 574.

52 Ibid. 574.

53 This interpretation is shared by Denni-Kenji Kipker and Friederike Voskamp, 'Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung' (2012) Datenschutz und Datensicherheit 737, 740; Peter Bräutigam and Florian Schmidt-Wudy, 'Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Article 15 der EU-Datenschutzgrundverordnung: Ein Diskussionsbeitrag zum anstehenden Trilog der EU-Gesetzgebungsorgane' (2015) Computer und Recht 56, 60.

54 Stiftung Datenschutz (n. 23) 6.

the European Union to consider the economic capabilities of the controller did not make the final cut of Article 20 GDPR.[55]

Let me add an interesting tidbit here: Google, Facebook, Apple, Microsoft and Twitter are engaged in the Data Transfer Project, which aims to create an open-source, service-to-service data portability platform.[56] The project's mission statement contains the following sentence: 'Companies have (for some reason) [sic!] all started offering their data in structured, commonly used and machine-readable formats, however in most cases those formats are not compatible with one another making it hard for users to re-import data they have exported.' This sentence reveals both the power and the shortcomings of Article 20 GDPR.

3. Inferences for businesses

What benefits would an Article 20-style rule bring to the B2B-context? Art. 20 GDRP contains a minimum requirement for the transmission of data that would help businesses switch data services. Apart from that, it is of little use to businesses, as they will regularly depend upon real-time access to the data.[57] Without such real-time access, neither an autonomous analysis nor the creation of aftermarket or complementary data-driven services seem feasible.[58] The transfer obligations under Article 20 GDPR therefore do not suffice for business purposes. Also, while the 'download your data' approach to portability may serve important data protection functions, businesses will most likely prefer a platform-model type of 'portability' which enables real-time data exchanges via APIs. Finally, as business data sets are exponentially greater than personal data sets, imposing a fee for the intermediate storage and/or transfer of the data might be adequate.

A key obstacle to expedient portability is interoperability. Machine-generated data is generally processed in specific proprietary data formats – even more so than personal data. However, it should be noted that several

55 Council of the European Union, '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)'(27 November 2015) Doc. 14481/15, 95.
56 <https://datatransferproject.dev> accessed 31 August 2020.
57 Schweitzer (n. 7) 574.
58 Schweitzer (n. 7) 574.

initiatives aim for inter-operability specifically for the industry 4.0.[59] If the law demands portability only where 'feasible', the law incentivises the development of proprietary data formats. But keep in mind that mandating interoperable standards may not only have beneficial effects on competition. The reverse may also be true: Interoperability may limit product design options and hamper innovation, may allow dominant market players to accrue even more data and may reduce network benefits for smaller players.[60] In trying to find middle ground, the law could require the provision of standardised retrieval software with respect to industry-specific data points.[61]

D. Conclusions and recommendations

I would hope that my conclusion is self-evident, but let me be clear:

Article 20 GDPR cannot serve as a blueprint for a business right to portability. It is rather of use to illustrate the pitfalls that need to be considered when creating any new portability right.

Any plan to introduce a portability right for businesses must be rooted in a clear policy objective. As such, different objectives come to mind: granting distributive justice to companies who contribute to a data value chain, preventing lock-in effects for small and medium enterprises, ensuring market efficiency by restraining dominating undertakings. The scope of the portability right as well as any exceptions and limitations must be

---

59 <https://opcfoundation.org>; <https://openindustry4.com>; <www.opengroup.org> all accessed 31 August 2020; cf. also Plattform Industrie 4.0, 'Shaping Industrie 4.0. Autonomous, interoperable and sustainable' (2019) 15–20 <www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/2019-progress-report.pdf?__blob=publicationFile&v=7> accessed 30 August 2020.

60 See the Memorundum on the Bill of the Federal Government for the reform of the German Act against Restraints of Competition: Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz) (9 September 2020) 89 <www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=6> accessed 15 September 2020; Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359, 1374.

61 Cf. US National Highway Traffic Safety Administration (NHTSA) rule 49 CFR Part 563 for the retrieval of event data recorders (in cars).

tailored towards this policy objective. Possibly, the solution does not lie in a one-size-fits-all norm, but in various more limited, but adequately tailored rules (that might even be industry-specific).

If the purpose of portability is to guarantee competition in data-driven aftermarket services or complementary products, then Article 20 GDPR does not provide an adequate model. However, Article 20 GDPR may be considered as a starting point for contractual portability rights, particularly regarding post-contractual transfer obligations. The introduction of such a contractual portability right to prevent lock-in effects certainly has its merits. The difficulties in defining such a right, however, are numerous and have been explained above.

In a European Union context, one also needs to be clear-eyed with respect to the possible harmonising gains of a contractual portability right. The harmonising effect of a non-mandatory contractual right may prove to be minimal, as businesses are bound to deviate by agreement from the rule. It is to be expected that repeat players will derogate from the portability rule in their standard terms and conditions. I include a gentle reminder that the approach to unfair contract terms in business contracts differs immensely amongst the Member States.[62]

In conclusion, let me emphasise that portability is an instrument and not a principle. Such an instrument needs a framework in which to flourish. The portability right created by Article 20 GDPR is embedded in the broader system of the GDPR. Whilst not all the provisions of the GDPR are crystal clear, the Regulation does provide a framework for the attribution of data, the legality of processing and the addressees of data subjects' rights. This framework is sorely missing for non-personal data. Any initiative to introduce a portability right for businesses must therefore first prepare the ground upon which the portability right might grow.

62 Cf. Alessio Zaccaria, 'Anmerkungen zur Umsetzung der Richtlinie 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen in Europa' (2016) Zeitschrift für Europäisches Privatrecht 159.