# Access to and porting of data under contract law: Consumer protection rules and market-based principles

*Axel Metzger*[*]

## *A. Introduction*

Is a party under a contract obliged to grant the other party access to data it has collected? From a contract law perspective, one is tempted to give the simple answer: 'Yes, if there has been an agreement that the party should have a right of access!' However, such an answer would seem too simplistic. Even though today's contract law is still based on the principle of freedom of contract, consumer protection and other policies (e.g. protection of employees, commercial agents, authors or other weaker parties) have changed its character. The present European contract law is permeated by mandatory provisions, information duties, correction mechanisms, default rules with regulatory objectives, procedural instruments and other kinds of rules which are meant to protect one contracting party from the other in asymmetric relationships. Therefore, the initial question must be raised in a more nuanced version: Is one party under a contract obliged to grant the other party access to the data it has collected even if the contract does not provide for such a right of access? Framed like this, the answer to the question will very much depend on the impact of the mentioned protective policies, especially consumer protection, on possible data access rights. It should be obvious that contract law is of main interest as a legal basis for access to data that has been collected within the contractual relationship. By contrast, any right of access to data collected outside of a contractual arrangement must be based on different legal grounds, e.g. data protection law, competition law, public sector information regulations. Such non-contractual legal grounds will only be taken into account for comparison in this chapter. The term 'access right' will be used in a broad sense, comprising both simple rights to access and also more technically demanding portability rights.

* The author would like to thank Lena Mischau, Heike Schweitzer, Herbert Zech and the participants of the Consumer Law Confernce 2019 for comments and discussions of the issues explored in this chapter.

## B. Consumer protection – Data access and porting under the DCSD

### I. Current state of the DCSD

The recent EU legislative package on consumer contracts – Directive 2019/770 on digital content and digital services (DCSD),[1] Directive 2019/771 on the sale of goods,[2] and Directive 2019/2161 on the modernisation of Union consumer protective rules ('Omnibus Directive')[3] – serves as a starting point for this chapter because the new Directives strive at reforming the regulatory framework for consumer contracts for the coming years if not decades. Therefore, one should search for contractual data access rights for consumers in this framework.

The DCSD with its focus on data-intensive e-commerce services is of major interest in this regard. The DCSD is applicable to a wide range of contracts for the supply of digital contents and digital services, including many Internet and social media services. It is applicable both to paid services and to services where consumers provide their personal data instead of a money consideration; see Article 3(2):

> This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

1 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] OJ L136/1.

2 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and Repealing Directive 1999/44/EC [2019] OJ L136/28.

3 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

Typical data-driven Internet services do not just process user data for the purpose of supplying the respective content or services or for compliance with legal requirements but also use such data for other purposes, namely for marketing and advertising, for market analysis, as training data for artificial intelligence tools etc. This is the very nature of today's data-driven business models. The rules of the DCSD will therefore apply to many of those contracts (but also to contracts with a money consideration), which raises the question whether consumers should have a right to access data collected in the course of these contractual relationships. The European legislature now has affirmed such a right in Article 16(2) DCSD with a reference to the General Data Protection Regulation (GDPR)[4] for personal data and in Article 16(4) DCSD with regard to non-personal data but only in case of a termination of the contract.

The Directive on the sale of goods does not provide a comparable rule for digital content, especially software, that is embedded in a physical product. Therefore, consumers will not have respective contractual data access rights with regard to devices used in the 'Internet of things'. This disparate approach has been criticised during the legislative process, but the legislature did not resolve the problem.[5] The Omnibus Directive is concerned with different matters and does not provide for additional access rights. The DCSD and the Directive on the sale of goods have to be transposed by the Member States by 1 July 2021. The new national contract law rules based on the two Directives will then apply from 1 January 2022.[6] For the Omnibus Directive, the implementation period runs until 28 November 2021. The new rules will then apply from 28 May 2022.[7] Germany has not yet published a draft proposal for the transposition of the three Directives into German law.

---

4 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.

5 See European Law Institute (ELI), 'Statement on the European Commission's proposed directive on the supply of digital content to consumers' (2015) 10–14, <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf> accessed 31 August 2020; Axel Metzger, Zohar Efroni, Lena Mischau and Jakob Metzger, 'Data-Related Aspects of the Digital Content Directive' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 90, paras 29–40.

6 Art. 24(1) DCSD; Art. 24(1) Directive on the sale of goods.

7 Art. 7(1) Omnibus Directive.

### II. Access to non-personal data under Article 16(4) DCSD

The DCSD provides for an access right of the consumer in the case of a termination of the contract. Article 16 DCSD stipulates the obligations of the trader in the event of termination. Paragraph 4 reads:

> Except in the situations referred to in point (a), (b) or (c) of paragraph 3, the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader.
> The consumer shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format.

The access right of Article 16(4) is bound to a number of conditions which, taken in sum, may reduce its scope of application to a large extent:

First, the access right of Article 16(4) only applies to 'content other than personal data, which was provided or created by the consumer'.[8] For personal data, the provisions of the GDPR take priority over the DCSD (Arts 3(8), 16(2) DCSD). Given the broad definition of personal data in Article 4(1) GDPR and the equally broad approach taken by the CJEU,[9] Article 16(4) has only limited practical value under the current circumstances.[10] As long as the service provider collects and processes data of a specific user who is identifiable by the (dynamic) IP address used during the visit to a website, such data is covered by the GDPR. This also holds true for any content that is created or uploaded by the user, e.g. texts, pictures, music or video files, digital goods in video games etc. Only when the contents or

8 The formulation has a tendency to exclude data derived or inferred by the trader; see 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, 1394.

9 See Case C-582/14 *Breyer* ECLI:EU:C:2016:779.

10 The extension to non-personal data is nevertheless supported in the literature; see Josef Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organisation BEUC' (BEUC 2018) 123–126, <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 31 August 2020; Ruth Janal, 'Data Portability – A Tale of Two Concepts' 8 (2017) Journal of Intellectual Property, Information Technology and E-Commerce Law 59, para. 35; Gerald Spindler, 'Die Richtlinie über Verträge über digitale Inhalte: Gewährleistung, Haftung und Änderungen' (2019) Multimedia und Recht 488, 492.

data are anonymised (if this is technically possible at all) may one consider applying Article 16(4) instead of the provisions of the GDPR. Also, one may discuss cases of consumers using anonymisation tools like VPN or TOR. However, the question then would be how to make and, if necessary, enforce a claim for access if the consumer wants to stay anonymous until she receives the content. It is therefore not surprising that commentators have difficulties giving concrete examples for the application of Article 16(4) DCSD.[11] But things may change in the future, especially if the principle of data minimisation in Article 5(1)(a) GDPR comes to be taken more seriously.

Second, the trader may refuse to grant access to the contents provided or created by the consumer if one of the situations described in Article 16(3)(a)-(c) is given. Under (a), the trader may deny any access if the 'content has no utility outside the context of the digital content or digital service supplied by the trader'. In this regard, it cannot suffice for the trader to assert that the content is of no such utility; rather, such utility should be assumed if the consumer claims to have an interest to use the content outside the context of the content or service. But even then, the trader may still argue that under (b) the content 'only relates to the consumer's activity when using the digital content or digital service supplied by the trader'. This proviso, if given a broad interpretation, could be used to undermine the access right significantly. All content stored on the trader's product or service 'relates to the consumer's activity'. Given the aim of Article 16(4), which is to not discourage the consumer from exercising the remedies of the DCSD and terminating a contract,[12] the proviso should be narrowed down to mere use data collected by the trader and to personalisation of the content or service made by the user,[13] whereas any content actively created or uploaded by the consumer should be subject to the access right.[14] Finally, according to (c) the trader may also refuse to grant access to content 'that has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts.' In this regard it has al-

11 But see Recitals 69, 71 DCSD. The former lists images, video and audio files as possible candidates for Art. 16(3), (4) without any discussion of the problem.

12 Recital 70 DCSD.

13 This second aspect is emphasised by Bernhard A. Koch, 'System der Rechtsbehelfe' in Wolfgang Stabentheiner, Christiane Wendehorst and Brigitta Zöchling-Jud (eds), *Das neue europäische Gewährleistungsrecht* (Manz 2019) 157, 178.

14 Interestingly, the proviso does speak of 'content' and not as in Art. 3(1)(2) of 'data'. This may be seen as a further argument that the portability right is not applicable to mere use data collected by the trader.

ready been stated that the proportionality requirement should be understood as explicitly obliging the supplier to configure its service in a way that allows contents to be extracted separately for each consumer. Service providers should apply state-of-the-art technology to protect the consumers' interest in their own contents. If suppliers do not set up their services in such a way as to facilitate the retrieval of consumers' content to the maximum effect possible according to state-of-the-art technology, they should not be heard with the argument of disproportionality.[15]

Third, the right of access under Article 16(4) DCSD is only applicable in case of termination of the contract, which limits its scope of application. Consumers who wish to use their contents on different services in parallel ('multi-homing'), e.g. playlists or search histories of music streaming services or sharing of photos and videos over social media platforms, may not rely on Article 16(4) DCSD. They must choose between the two services, terminate one of the contracts, claim for access under Article 16(4) DCSD and then port their contents to the other service. Moreover, Article 16(4) is only (directly) applicable in case of a termination which is based on a failure to supply by the trader or the lack of conformity or in case of modification of the content or service in accordance with Article 19. All other grounds of termination, especially the right to terminate long-term contracts after a certain period of time,[16] are outside the scope of the DCSD. However, Member States are free to expand the portability right to such situations.[17]

If all conditions are fulfilled, the consumer 'shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format', under Article 16(4)(2). The DCSD thus does not just provide a simple right of access but a more advanced right of portability. If the consumer receives the contents in a commonly used and machine-readable format, it should be possible for competing services to offer the necessary interfaces and to help the consumer to port the contents.

---

15 See Metzger and others (n. 5) para. 54.

16 See Annex 1(h) Unfair Terms Directive (EEC) 93/13 and, as an example, the German implementation in Sec. 309(9)(a) German Civil Code (*Bürgerliches Gesetzbuch*) (preclusion of termination in general terms for more than two years is void). Compare Wolfgang Wurmnest, in *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, C.H. Beck 2019) § 309 Nr. 9 paras 2–4.

17 The full harmonisation approach does not cover other grounds of termination; see Art. 3(10), Recitals 11, 12 DCSD.

Like all consumer rights of the DCSD, Article 16(4) is of a mandatory nature; see Article 22(1). However, the trader may specify the conditions of the right of access as long as these conditions do not deviate from Article 16(4) to the detriment of the consumer (Article 22(2)). One may justify this strict regulatory approach by multiple market failures, ranging from the (general) asymmetry between consumers and professionals[18] to the dysfunctional competition on some of the markets for digital services caused by network effects[19] to the threat of lock-in effects.[20] These market failures are amplified by cognitive biases of consumers, who overvalue short-term benefits from services over long-term risks.[21]

### *III. Comparison of Article 16(4) DCSD and Articles 15, 20 GDPR*

Consumer claims for access to personal data can only be based on the provisions of the GDPR, irrespective of whether the controller has concluded a contract on the supply of a digital good or digital service with the consumer or not. Article 16(4) DCSD excludes claims for access to personal data, Article 3(8) clarifies that 'Union law on the protection of personal data shall apply to any personal data processed in connection with contracts referred to in paragraph 1'. The access rights of the GDPR are of a different

---

18 Shmuel I. Becher, 'Asymmetric Information in Consumer Contracts: The Challenge That Is Yet to Be Met' (2008) 45 American Business Law Journal 723, 728, 733–35; Holger Fleischer, *Informationsasymmetrie im Vertragsrecht* (C.H. Beck 2001) 203–08, 570–72; Giesela Rühl, 'Consumer Protection in Choice of Law' (2011) 44 Cornell International Law Journal 570, 571–595.

19 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era – Final report' (2019) 4–5, <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 31 August 2020.

20 Ibid. 34.

21 The bias has been described for free services offered in exchange for personal data. See OECD, 'Big data: Bringing competition policy to the digital era: Background note by the Secretariat' (November 2016) para. 91, <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> accessed 31 August 2020: 'The user is given the immediate benefit of the zero-price service, but is unaware of the short or long-term costs in divulging information, as they do not know how the data will be used and by whom.' See also Cory Hallam and Gianluca Zanella, 'Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards' (2017) 68 Computers in Human Behavior 217; Yoan Hermstrüwer, *Informationelle Selbstgefährdung* (Mohr Siebeck 2016) 93ff. The argument should apply similarly for non-personal data provided by consumers in ignorance of the long-term disadvantages.

nature. Their aim is not to balance the interests of contracting parties but to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.[22]

The GDPR recognises a general right of access in Article 15 and a more specific right to data portability in Article 20. The right of access in Article 15 is broader in scope.[23] It covers not just the data processed by the controller but also additional information with regard to the processing, ranging from (a) the purpose of processing to (h) the existence of automated decision-making, including profiling. Article 15 GDPR is not limited to specific legal grounds of the processing. However, the controller has only limited obligations on the format of the information, which must be provided according to paragraph 3 in a 'commonly used electronic form'. Article 20 GDPR is more limited in scope. It is only applicable to data that the data subject 'has provided to a controller'.[24] Also, Article 20 GDPR requires that the 'processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1).'[25] But the rights of the data subject under Article 20 GDPR are more extensive. Under Article 20 GDPR, the data subject cannot just ask for the disclosure of the processed personal data but for a transmission 'in a structured, commonly used and machine-readable format'. The data subject has the right to 'transmit those data to another controller without hindrance from the controller' and even ask the data controller to transmit the data directly to another controller, 'where technically feasible' (Article 20(2)). The porting of data may be combined with a claim to erase all data stored by the controller (Article 20(3)). However, the rights and freedoms of third parties may not be affected by any access to or porting of data, according to Articles 15(4) and 20(4) GDPR.[26]

22 Recital 1 GDPR.

23 Drexl (n. 10) 151.

24 For a broad interpretation see Janal (n. 10) para. 9: Right to portability extends to data provided by the consumer's conduct and use of gadgets or services. See also Drexl (n. 10) 152: Right extends to 'observed' data.

25 For an application of Art. 20 GDPR with regard to illegally processed data Janal (n. 10) para. 11; see also Drexl (n. 9) 153.

26 Art. 20 is lex specialis to Art. 15 if the data subject requests their personal data in a 'structured, commonly used and machine-readable format' or if a transmission to another controller is requested; see Lorenz Franck in Peter Gola, *Datenschutz-grundverordnung* (2nd edn, C.H. Beck 2018) Art. 15 para. 4. However, if the data subject requests the additional information listed at the end of Art. 15(1) GDPR, then this provision is lex specialis to Art. 20 GDPR.

The access rights of the GDPR are broader in scope and more favourable to consumers than Article 16(4) DCSD in many respects. They do not require the conclusion and later termination of a contract. Article 20 (but not Article 15) GDPR provides for more advanced requirements with regard to the format of the data ('structured') and grants the right to transmit the data received or to request a direct transmission from one controller to another controller. Both Articles 15 and 20 GDPR are not bound to restrictive conditions comparable to Article 16(3) DCSD[27] but provide for a reservation for the rights and freedoms of third parties. Article 15 GDPR (but not Article 20) is applicable to any data processed by a controller, plus additional information on the processing, irrespective of the legal basis of such processing.

In sum, one may regret the inconsistencies and unintentional differences between the legal regimes for access and porting of non-personal contents under Article 16(4) DCDS and personal data under Articles 15, 20 GDPR. However, the underlying pattern to leave the rules of the GDPR untouched by the DCSD serves the goal of coherence in this regard.[28] Moreover, it is plausible to grant more far-reaching access rights with regard to personal data: Article 16(4) DCSD is primarily concerned with consumer rights (with a pro-competitive side-effect); by contrast, Articles 15, 20 GDPR protect fundamental rights (also with a pro-competitive side-effect).[29]

### *IV. Individual and collective enforcement*

The remedies for consumers under the DCSD are drafted as individual claims. This is also the case for Article 16(4) DCSD, which obliges the trader to grant access to contents 'at the request of the consumer'. Courts and data protection supervisors are still in an experimental stage with individual rights of access to personal data under the GDPR.[30] Data protection law

27 Critical Janal (n. 10) para. 10: proportionality should also apply with regard to Art. 20 GDPR. See also Drexl, (n. 10) 152.

28 See Metzger and others (n. 5) para. 54.

29 Janal (n. 10) paras 4, 5 with further references.

30 See Stefan Brink and Daniel Joos, 'Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie' (2019) Zeitschrift für Datenschutz 483; Niko Härting, 'Was ist eigentlich eine "Kopie?"' (2019) Computer und Recht 219; see also *Dawson-Damer v. Taylor Wessing LLP* [2017] EWCA Civ 74 (16 February 2017) on the Data Protection Act 1998.

in general suffers from private enforcement in legal practice. It is thus for good reasons that Article 21(2) DCSD allows collective enforcement, as determined by national law, by (a) public bodies or their representatives, (b) consumer organisations having a legitimate interest in protecting consumers, (c) professional organisations having a legitimate interest in acting, and (d) not-for-profit bodies, organisations or associations active in the field of the protection of data subjects' rights and freedoms as defined in Article 80 GDPR.[31]

Besides these collective entities, it will be a question of special interest in Germany whether competitors may raise claims based on unfair competition if their competitors do not make available contents provided or created by the consumers in compliance with Article 16(4) DCSD. Germany has a broad practice of private enforcement of public and private law regulations by means of unfair competition law.[32] According to Section 3a Act against Unfair Competition, competitors may bring claims based on the breach of law 'where a person violates a statutory provision which is also intended to regulate market conduct in the interest of market participants and the breach of law is suited to appreciably harming the interests of consumers, other market participants and competitors.' German courts have allowed such claims for a variety of provisions, including provisions of the Consumer Sales Directive (EC) 1999/44,[33] the Unfair Terms Directive (EC) 93/13[34] and some provisions of the pre-GDPR German Federal Data Pro-

31 Art. 21(2)(d) DCSD does not specify whether such organisations may only enforce rights grounded in data protection law or whether they may also enforce claims arising from contract law. One may argue for the latter approach with the position of the rule in the DCSD, which provides only contractual remedies and leaves the data protection issues to the GDPR. Limiting the scope of Art. 21(2)(d) DCSD to claims from the realm of data protection law would reduce its scope of application to zero. Still, the mandate of such organisations may be limited by their own by-laws to data protection law.

32 On the compliance of this practice with Directive (EU) 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22, see Axel Metzger, 'Die Entwicklung des Rechtsbruchtatbestands nach der Umsetzung der UGP-Richtlinie – ein Zwischenbericht' (2015) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 687.

33 German Federal Supreme Court (*BGH*), 31 March 2010, Case I ZR 34/08 (2010) Gewerblicher Rechtsschutz und Urheberrecht 1117 – *Gewährleistungsausschluss im Internet*.

34 German Federal Supreme Court (*BGH*), 31 May 2012, Case I ZR 45/11 (2012) Gewerblicher Rechtsschutz und Urheberrecht 949 – *Missbräuchliche Vertragsstrafe*.

tection Act[35] and now also of the GDPR.[36] It is thus a realistic scenario that some of the provisions of the DCSD including Article 16(4) will also be characterised as provisions intended to regulate market conduct in the interest of consumers. The consequence would be that competitors could indirectly claim violations of Article 16(4) through the backdoor of unfair competition law. This would also permit them to send cease-and-desist letters and to claim for recovery of their expenses according to Section 12(1)(2) Act against Unfair Competition, an enforcement mechanism which has turned out to be very effective in some areas, but which may also be abused as a (lawyer's) business model.

### *V. Transfer or fiduciary exercise of rights*

A different approach to strengthen the enforcement of portability claims under Article 16(4) DCSD would be to allow for their transfer to other providers of digital contents or services. If such providers were allowed to acquire portability claims of users against their old service providers, they could enforce those rights and claim for a direct transmission of the contents from the old service provider to their database, e.g. Flickr could ask Apple for a direct transmission of pictures stored on a cloud, Soundcloud could claim for playlists and search history to be transmitted by Spotify etc. – based on the premise that these contents would be non-personal data and covered by Article 16(4) DCSD. Such an approach could boost the enforcement of portability claims. The incentive for the new provider to enforce such claims would be higher than for the individual user, since it would permit the provider to win new customers and not, as in the case of

35 On Sec. 28 (pre-GDPR) German Federal Data Protection Act, see Cologne Higher Regional Court (*Oberlandesgericht Köln*), 17 January 2014, Case 6 U 167/13 (2014) Beck-Rechtsprechung 07826 – *Unzulässige Datenverwendung zur Mandatsakquise-Anlegerbrief*; Karlsruhe Higher Regional Court (*Oberlandesgericht Karlsruhe*), 9 May 2012, Case 6 U 38/11 (2012) Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report 396 – *Werbung nach Versorgerwechsel*. But see also Munich Higher Regional Court (*Oberlandesgericht München*), 12 January 2012, Case 29 U 3926/11 (2012) Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report 395 – *Nutzung von Daten ehemaliger Gaskunden*.

36 See Hamburg Higher Regional Court (*Oberlandesgericht Hamburg*), 25 October 2018, Case 3 U 66/17, (2019) Gewerblicher Rechtsschutz und Urheberrecht 86 – *Allergenbestellbögen*. The question of whether this practice is compatible with the GDPR has just recently been referred to the CJEU: see German Federal Supreme Court (*BGH*), 28 May 2020, Case I ZR 186/17.

the individual user, to port his or her user-generated contents from a poorly performing service to another functionally equivalent and hopefully satisfactory service. Also, transaction costs would be lower; providers would implement standardised claim-enforcement mechanisms and profit from the economy of scales. If the transfer were only allowed as part of a contract on digital contents or services with the new provider, the consumer would profit from such an arrangement. The new provider would release the consumer from enforcing the portability claim against the old provider without the risk of a later transfer of his claims to third parties. As an additional safeguard, one could allow such a transfer strictly on condition that the new provider has a duty to enforce the portability claim.

The DCSD does not preclude such a transfer. A transfer to a new provider would not lead to a derogation from the provisions of the DCSD 'to the detriment of the consumer' in the sense of Article 22(1) DCSD.[37] Rather, it would help to strengthen the impact of the portability rules. Also, a transfer would not conflict with the principle of inalienability of personality rights,[38] since Article 16(4) is only concerned with non-personal contents. Consumers, moreover, would have a mandatory portability right against the new provider under Article 16(4) DCSD once the contents have been transferred. The transfer would therefore not lead to a situation in which the consumer would lose any right against the new provider.

However, if a transfer of the portability claim is still seen as a too far-reaching disposition of mandatory consumer rights, one could instead use instruments like fiduciary entitlements or authorisations that allow the new provider to exercise the portability claim in the name of the con-

37 Art. 22 DCSD restricts contractual arrangements between the consumer and the (old) service provider but does not explicitly restrict such arrangements with third parties. However, such agreement could still be seen as an indirect derogation or variation of the mandatory consumer rights. See on the parallel provision in Art. 7 Consumer Sales Directive (EC) 1999/44 and the German implementation in Sec. 476 German Civil Code Florian Faust, in *Beck Online-Kommentar zum BGB* (53rd edn, C.H. Beck 2020) § 476 para. 11; Stefan Lorenz in *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, C.H. Beck 2019) § 476 paras 7, 33.

38 This principle is known, inter alia, in German and French law, though with many nuances and exceptions; see Huw Beverley-Smith, Ansgar Ohly and Agnès Lucas-Schloetter, *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation* (CUP 2005) 129–138, 194–95 with further references.

sumer.[39] Such an entitlement or authorisation could suffice to enable the party with the highest incentive to enforce portability claims directly.

## C. Data access and porting under general contract law principles

### I. No mandatory access rules in European and German general contract law

#### 1. European contract law

The analysis so far has shown that EU law grants to consumers (and data subjects) access and portability rights both for personal data under Articles 15, 20 GDPR and for other data under Article 16(4) DCSD. Yet it has also become clear that these European consumer (or data subject) rights are not without gaps, especially with regard to embedded contents under Directive (EU) 771/2019 on the sale of goods but also with regard to the portability of data in the case of regular termination of long-term contracts, which is not covered by Article 16(4) DCSD.

A much broader gap, however, exists with regard to business-to-business (B2B) contracts. Access to and portability of data are of major importance in B2B contractual relationships. Professional users of digital services, e.g. cloud services, business platforms and software tools, have a vital interest to obtain access to contents and data they have stored or processed on these services or platforms or which they have produced with these software tools. Such data may have been actively uploaded to or produced with the service, platform or tool. But data may also be based on an observation or profiling of the business customer's activities. Businesses do also have an interest to access data that their contracting parties have derived from original raw data produced by the customer. In addition, data embedded in machines and other (tangible) devices is of enormous economic importance for both contracting parties, including data processed and recorded in airplanes (both for the manufacturer and the airline), in agricultural machines (both for the farmer and the producer of the machine, but also third parties, e.g. for providers of information services on the cli-

39 Such a specific fiduciary entitlement would not replace the more general idea of establishing general data fiduciaries or personal information management systems (PIMS) as neutral entities which administer the personal data in the interest of the provider's customers; see European Data Protection Supervisor, Opinion 9/2016 on Personal Information Management Systems, <https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf> accessed 31 August 2020.

mate, producers of seed or fertilisers or herbicides) or in wind power stations (both for the owner of the station and the producer).

The few as yet existing mandatory B2B data access or portability rights under EU law are not to be qualified as contract law rules. They are of a different nature, namely general competition law under Article 102 TFEU,[40] or relate to more specific regulatory regimes like the EU rules on access to vehicle repair and maintenance information under Regulation 715/2007,[41] the EU rules in the banking sector under the Payment Services Directive 2015/2366[42] and the EU rules on access to data of 'smart meters' for electricity and natural gas under Directives (EU) 2009/73 and 2019/944.

In the area of contract law, the European Commission by now has published a number of soft law instruments defining principles on data-sharing between businesses (B2B) and between businesses and governmental authorities (B2G) and describing different models of data sharing with a number of examples.[43] The principles explained in the instruments, 'transparency', 'shared value creation', 'respect for each other's commercial interests', 'undistorted competition', and 'minimised data lock-in', should indeed guide every contractual relationship. But one should not be surprised that market actors do not always follow these principles but rather seek to maximise their profit. One may describe these statements of principles either as toothless or as market-oriented and liberal, depending on the observer's perspective.

The – more general – soft law instruments of the European Commission have been complemented with specific duties for 'online mediation ser-

40 See Heike Schweitzer and Robert Welker, 'A legal framework for access to data – A competition policy perspective', in this volume.

41 Arts 6–9 Regulation (EC) No. 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance data [2007] OJ L171/1; see on this Wolfgang Kerber and Daniel Gill, 'Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 244–257.

42 Arts 38–60 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.

43 See Communication of the European 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 and European Commission Staff Working Document, 'Guidance on sharing private sector data in the European data economy' SWD(2018) 125 final.

vices' by the Fairness and Transparency Regulation (EU) 2019/1150.[44] The Fairness and transparency Regulation targets online sales platforms like Amazon. The Regulation does not oblige those platforms to grant their business users access to personal or other data which the users of the platform provide for their use or which is generated by the platform. However, the Regulation puts the platforms under an obligation to provide their business users 'in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data',[45] and moreover to provide a description of 'any differentiated treatment which they give, or might give, in relation to goods or services offered to consumers through those online intermediation services by, on the one hand, either that provider itself or any business users which that provider controls and, on the other hand, other business users', including the 'access that the provider, or that the business users or corporate website users which that provider controls, may have to any personal data or other data' and the 'access to, conditions for, or any direct or indirect remuneration charged for the use of services or functionalities, or technical interfaces, that are relevant to the business user or the corporate website user and that are directly connected or ancillary to utilising the online intermediation services or online search engines concerned.'[46] These information duties are supplemented by a specific right of access to data in case of a restriction or termination and later reinstatement of the online mediation service.[47] The Fairness and Transparency Regulation, however, does not introduce any further mandatory or default access rights. As such, it will strengthen transparency with regard to the existence or non-existence of contractual data access rights for the specific case of 'online mediation services' but it is far from establishing a general right of access or portability to data in B2B relationships.

The recently published 'European strategy for data' of the European Commission seems to follow the cautious approach of the last years with

44 The Regulation applies also to online search engines: see Art. 1(1) Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57. However, the provisions of interest in this paper are only applicable to online mediation services.

45 Art. 9 Regulation (EU) 2019/1150.

46 Art. 7(1), (3)(a) and (d) Regulation (EU) 2019/1150.

47 Art. 4(3) Regulation (EU) 2019/1150.

regard to B2B contracts.[48] The strategy paper emphasises the vision to create a European data space where data can flow within the EU across sectors and addresses the problem that 'data sharing between companies has not taken off at sufficient scale'. However, the measures announced, especially the 'Data Act (2021)', seem to follow a market-based approach for B2B contracts: 'The general principle shall be to facilitate voluntary data sharing.' And: 'only where specific circumstances so dictate, access to data should be made compulsory'.[49]

In sum, EU contract law legislation so far does not provide for a general right of access or portability of data with regard to B2B relationships. Yet one may ask whether such a right may be inferred from general principles of contract law, such as the Principles of European Contract Law (PECL), the Unidroit Principles or the Draft Common Frame of Reference (DCFR). Starting points for such access rights could be information duties, implied terms or restitution rights in case of termination of contract. However, the collections of principles, at least for the most part, contain principles of a non-mandatory nature.[50] They do not provide for any mandatory access rights.

### 2. *National contract law – The case of Germany*

On the national level, again one may use different legal doctrines of general contract law to construe access rights. With regard to information duties inferred from the principle of good faith and fair dealing, contract law traditions of EU Member States differ significantly. Some states follow a tradition in which one contracting party, at least to a certain extent, is responsible for the well-being of the other party, whereas other jurisdictions emphasise the principle of self-responsibility. Yet the differences should also not be overemphasised. Comparative analysis of concrete cases shows that

48 Communication of the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 'A European strategy for data' COM(2020) 66 final.

49 Ibid. 13.

50 See Art. 1:102(2) Principles of European Contract Law (PECL), but see also Art. 1:201 PECL (good faith and fair dealing mandatory); Art. 1.5 Unidroit Principles 2016, Art. II.1:102(2) Draft Common Frame of Reference (DCFR).

apparently divergent traditions come to surprisingly consistent judgments.[51]

German law is well known for its strong emphasis of the principle of good faith.[52] German judiciary and doctrine have developed a variety of information duties and other implied secondary obligations of the parties to a contract.[53] However, any of the so far recognised duties of one party to disclose information to the other party to the contract are highly case-specific. Therefore, one might well expect that German courts would grant access rights in specific cases under the guiding principle of good faith. But this approach would certainly not lead to a general right of access and portability in B2B contracts. Also, information duties are not per se of a mandatory nature. Still, one could consider examples of access rights based on such general information duties. If for example the owner of an industry machine needs certain data for the maintenance of the machine one could consider such a right of access, at least in cases in which the producer does not offer maintenance services. To give a second example: A customer of a cloud service should certainly have a right to access the data and content stored on the cloud server during the contract and after its termination. The Higher Regional Court of Munich derived such a right of access as an implied term from the principle of good faith and obliged the service provider, after termination of the contract, to support the customer in the porting of its data to a different service provider.[54]

Besides information duties and implied terms, courts could also consider other legal doctrines of contract law as legal grounds for access rights. Depending on the concrete nature of the rights and duties of the parties to the contract, provisions from the specific contracts section of the German Civil Code (BGB) could be applicable. According to Section 667 BGB, in the case of a contract of mandate, 'the mandatary is obliged to return to the mandator everything he receives to perform the mandate and what he obtains from carrying out the transaction.' The concept of mandate (in-

51 Cf. Reinhard Zimmermann and Simon Whittaker (eds), *Good Faith in European Contract Law* (CUP 2000) 653.

52 See Sec. 242 German Civil Code (performance in good faith): 'An obligor has a duty to perform according to the requirements of good faith, taking customary practice into consideration.'.

53 The concept of implied secondary obligation is today codified in Sec. 241(2) German Civil Code: 'An obligation may also, depending on its contents, oblige each party to take account of the rights, legal interests and other interests of the other party.'.

54 Munich Higher Regional Court (*Oberlandesgericht München*), 22 April 1999, Case 6 U 1657/99, (1999) Computer und Recht 484, paras 179–186.

cluding paid management of the affairs of another, Section 675 German Civil Code) is broad and could also cover, eg, escrow agreements or agreements on the data processing on behalf of a controller in the sense of Article 28(1) GDPR.[55] However, Section 667 German Civil Code can be waived.[56] In the case of a contract on safekeeping, according to Section 695 German Civil Code, 'the depositor may at any time demand that the thing deposited is returned, even if a period for safekeeping has been specified.' It has been suggested that (at least certain) cloud service contracts be characterised as safekeeping contracts.[57] If the provisions on safekeeping contracts were applicable here, it would still be controversial whether the parties were allowed to exclude the right to claim for return according Section 695 German Civil Code.[58]

Finally, rights and duties in case of termination of a contract could provide a basis for access claims. The basis for such claims could be found in the general contract termination rules, especially Section 346(1) German Civil Code: 'If one party to a contract has contractually reserved the right to revoke or if he has a statutory right of revocation, then, in the case of revocation, performance received and emoluments taken are to be returned.' This could justify a claim by one contracting party against the other contracting party to return data or content transmitted or collected during a contract, e.g. if a buyer of a machine revokes the contract after some months because of lack of conformity and requests access and transmission of valuable data collected and stored by the machine.[59] However, Section

55 See for further examples Marc Strittmatter, in Fabian Schuster and Malte Grützmacher (eds), *IT-Recht Kommentar* (Beck 2020) § 675 BGB paras 17–24. See for a client's access claim to data stored by a tax consultant German Federal Supreme Court (*BGH*), 11 March 2004, Case IX ZR 187/03, (2004) Neue Juristische Wochenschrift Rechtsprechungs-Report Zivilrecht 1290.

56 Detlef Fischer in *Beck Online-Kommentar zum BGB* (53rd edn, C.H. Beck 2020) § 667 para. 5.

57 See, for example, Martin Henssler in *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, C.H. Beck 2020) § 688 para. 9; Frank A. Koch, 'Application Service Providing als neue IT-Leistung' (2001) Der IT-Rechtsberater 39, 42.

58 See Henssler (n. 57) § 695 para. 2 with further references.

59 This would require characterising the active provision of data by the buyer or the passive acceptance of data collection by the seller as the performance of an explicit or implied secondary obligation of the buyer under the contract, the value of which would then be returned in accordance with Sec. 346(1)(1), (2) German Civil Code, cf. German Federal Supreme Court, 28 November 1997, Case V ZR 178/96, (1998) Neue Juristische Wochenschrift 1079, 1080–81. On the application of Sec. 346(1) German Civil Code in case of provision of data as performance, see

346 BGB can be modified and even excluded by the parties.[60] It does not provide a basis for mandatory access rights. Also, Section 346 is not applicable in case of termination of a long-term contract.[61] In this regard, a claim based on unjust enrichment in accordance with Section 812(1)(1) BGB could be considered.[62]

To sum up, German law of contracts does not provide for a general access right to data transmitted, created or observed by contracting parties, be it during the contractual relationship or after its termination. The existing information, access and return duties are case-specific and for the most part of a non-mandatory nature. This makes it clear that there will be no legal ground for access claims in many cases without explicit contract provision and without the special circumstances of good faith etc. discussed above, e.g. no contractual data access right for airlines or farmers covering data processed and recorded in airplanes or agricultural machines etc.

### *II. A case for mandatory access rules in B2B contracts?*

European and German contract law do not provide for a general mandatory access and portability right that would also be applicable in B2B contracts. Whether it should provide for such access rights is a question of politics, which however should try to back its arguments with findings from law and economics research. From this perspective, the starting point is a market model where perfect competition and freedom of contract lead to an allocation of goods, here the data in question, to the market actor who can maximise welfare out of the use of this good.[63] Unfortunately, markets are not always fully functioning. The allocation mechanisms of markets

---

Axel Metzger, 'Dienst gegen Daten: Ein synallagmatischer Vertrag' (2016) 216 Archiv für die civilistische Praxis 817, 861.

60 See Reinhard Gaier, in *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, C.H. Beck 2019) § 346 para. 1.

61 Ibid. para. 17.

62 Sec. 812(1)(1) German Civil Code: 'A person who obtains something as a result of the performance of another person or otherwise at his expense without legal grounds for doing so is under a duty to make restitution to him.' However, such a claim would be of a non-contractual nature.

63 This is a very basic assumption of every welfare economics model since Adam Smith's famous 'invisible hand' theorem; see Adam Smith, *An inquiry into the nature and causes of the wealth of nations* (The Modern Library 1937) 423. See also Robert B. Cooter and Thomas Ulen, *Law and Economics* (6th edn, Pearson 2014) 275–279.

are often distorted. Based on this premise, the research on law and economics refers to different kinds of market failures as justification for state intervention.[64] A first reason to intervene in B2B markets is lack of competition. But other market failures, namely asymmetries of information or negative externalities, may also call for state intervention. Moreover, state regulation may be helpful to safeguard legal certainty and lower transaction costs.

The clearest case for a possible failure of data markets concerns negative externalities caused by data access rights. If the data in question is personal data in the sense of the GDPR, any access granted to third parties causes negative externalities with regard to the data subjects. This risk, however, is ruled out to a large extent by the GDPR. Any granting of access to personal data fulfils the definition of a 'processing of data' in the sense of the GDPR[65] and as such requires a justification in accordance with Article 6 GDPR. Violation of the requirements of the GDPR is sanctioned by severe penalties. It is evident that the current European law is torn between a strong data protection policy and the wish to stimulate the European digital economy by encouraging data sharing.

With regard to lack of competition as a market failure, the situation is less evident. Obviously markets for digital goods and services have a tendency to concentrate on a small number of competitors. In particular, some Internet services function as platforms for their different kinds of users and have as such a natural inclination towards dominance.[66] Network effects push consumers and businesses to become the customers of highly centralised communication or trading platforms. Once services have established a dominant position in one market, they might leverage their market power to closely related markets. These effects may be reinforced by lock-in effects that prevent users from changing from one service to another. Competition law nevertheless so far has difficulties remedying those problems, especially when service providers grow into a dominant

64 See Steven Shavell, *Foundations of Economic Analysis of Law* (Harvard University Press 2004) 320–22; Hans-Bernd Schäfer and Claus Ott, *Lehrbuch der ökonomischen Analyse des Zivilrechts* (5th edn, Springer 2012) 78–81; Cooter and Ulen (n. 63) 286–291.

65 Art. 4(2) GDPR: 'disclosure by transmission, dissemination or otherwise making available'.

66 On the following see Crémer, de Montjoye and Schweitzer (n. 19) 19ff.; Lena Mischau, 'Market Power Assessment in Digital Markets – A German Perspective' (2020) GRUR International – Journal of European and International IP Law 233–248.

position.[67] But is it the right answer to intervene in these markets with mandatory contract rules, more specifically with mandatory access and portability rights to overcome, at least, the mentioned lock-in effects? There are good arguments to answer the question in the affirmative, at least for service providers with a dominant market position or in other cases of restraints of competition.[68] But the situation is different if the user has a choice between several services and may compare access and portability rules before entering into a contract. In a market with competition, a professional user should be in a position to choose the service with the preferred access rules. And if, as a consequence of competition, this feature turns out to be of importance for the customer's choice, the service providers should react to this demand.[69] Therefore, prevention of lock-in effects is indicated in markets with dominant actors but less evident for other situations. A mandatory access and portability rule that is applicable to all B2B contracts and does not require such a dominant position would most likely overshoot the mark. General access rules could be used by already dominant companies to gather data stored by other market actors, e.g. aircraft manufacturers could claim for access to data collected by airlines in their own monitoring devices. Access and portability rules could also be used to incentivise customers of smaller competitors to switch to

67 The currently pending Legislative draft for a 10th revision of the German Act against Restraints of Competition tries to introduce new instruments or up-date existing ones, especially Sec. 18(3b): Intermediation power; Sec. 19a: Paramount cross-market importance for competition; Sec. 20(1) and (1a): Relative market power; see the Government Bill for the 10th revision: 'Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz)' (9 September 2020) <www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=6> accessed 15 September 2020. On the whole, see Mischau (n. 66) 246–248. See also the recent decision German Federal Supreme Court (BGH), 23 June 2020, Case KVR 69/19 (2020) 51 International Journal of Intellectual Property and Competition Law (forthcoming) (English translation) – *Bundeskartellamt/Facebook* (not yet published).

68 See Josef Drexl, 'Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz' (2017) Neue Zeitschrift für Kartellrecht 415, 418; Axel Metzger, 'Mehr Freiheit wagen auf dem Markt der Daten: Voraussetzungen und Grenzen eines Marktmodells für "big data"' in Anatol Dutta and Christian Heinze (eds) *Mehr Freiheit wagen – Symposium zur Emeritierung von Jürgen Basedow* (Mohr Siebeck 2018) 131, 144–45.

69 If all competitors exclude access, one should the raise the question if the market is fully functioning or if competition law must intervene.

larger competitors on cloud markets. Moreover, claims for access to data may arise out of contractual relationships, e.g. if an independent flight-tracking service seeks access to data collected by aircrafts. In such a case, no pre-existent contract can be supplemented by mandatory (or implied) duties but a regulatory intervention would have to create a right of access on a direct statutory basis. Therefore, legislatures should only introduce contractual access rights based on lack of competition if competition law requires such rights. In this case, the remedy to cure the competition law issue can be an intervention with mandatory rules for contracts, e.g. access to and porting of data. But such an approach should be justified by a clear indication of competition law. Still, this reluctance towards general access rules for B2B contracts should not preclude court intervention if a lock-in situation is abused by the service provider in a concrete case, e.g. if a denial of access would be against good faith given the concrete contractual arrangement and the circumstances of the case.[70]

Another consideration to justify data access rights in B2B contracts could be found, at least at first glance, in the different theories of asymmetric information in contract negotiations.[71] It may appear as intuitive to discuss the access to data cases along the lines of the different information disclosure doctrines known in many jurisdictions, according to which one party to a contract may have a duty to disclose information during the negotiation of the contract. Economic analysis of law has developed several approaches to explain these doctrines and to identify their limits. However, on closer scrutiny, the cases in which disclosure duties are seen as necessary to remedy asymmetric information concern situations different from the claims for access discussed here, especially if the buyer or seller of a commodity possesses information that is relevant for the contract with regard to the price paid for the commodity, e.g. if the basement of a home leaks or if a property bears minerals or oil. Here it may be socially desirable or not that information be disclosed with regard to factors[72] like who controls the information – the buyer or the seller – and who can make more socially valuable use of the information, which party can provide the information at which costs, whether the incentive to acquire the information would be undesirably reduced by a disclosure obligation or whether the information is socially valuable or has only private use. Those cases and cri-

70 Compare Munich Higher Regional Court (*Oberlandesgericht München*), 22 April 1999, Case 6 U 1657/99, (1999) Computer und Recht 484, paras 179–186.

71 See for a comprehensive comparative legal and economic analysis Fleischer (n. 18) passim. See also Cooter and Ulen (n. 63) 289–90; Shavell (n. 64) 331–335.

72 See Fleischer (n. 18) 175–177, 1000–1001; Shavell (n. 64) 332–334.

teria concern disclosure obligations relevant for the determination of the price of a commodity or service during the contract negotiation stage. They do not concern possible access rights with regard to data collected and processed in the course of a contract. Here, the information itself is the asset that should be allocated efficiently by the mechanisms of the market.[73] It would be an oversimplification to infer an information asymmetry to be remedied by state intervention from the fact that one party has an asset, here data, which the other party has not. Interestingly, the recently adopted Fairness and transparency Regulation does not oblige platforms to grant its business users access to personal or other data but mainly provides a duty to disclose whether the platform grants access to data and under which conditions. In the legal literature, additional information duties for B2B contracts have been suggested, in particular in regard of the general information of whether the other contracting party has collected data and what data has been collected and processed.[74]

To sum up, based on the established models of economics analysis of contracts, one can hardly justify general mandatory access and porting rules for data collected and processed by one of the contracting parties during a B2B contract. In situations of restraints of competition, competition law may require certain limits of party autonomy which may come along as mandatory rules for contracts; but such rules must be clearly justified on a competition law basis. With regard to information asymmetries, it may be useful to implement information duties with regard to the data collected and processed and, if applicable, to the conditions of access. However, the economics of information so far have not revealed a clear case for a general right of access to data.

### *III. Access and porting as default rules for B2B contracts?*

#### *1. Concept and functions of default contract rules*

Given that most provisions of contract law are of a non-mandatory nature, it may be more intuitive to ask whether European or German contract law should implement default rules on data access and porting for B2B contracts.

---

73 See Herbert Zech, *Information als Schutzgegenstand* (Mohr Siebeck 2012) 152–57.
74 Drexl (n. 68) 418; Metzger (n. 68) 151–52.

The starting point for such an approach is the theory of incompleteness of contracts.[75] Contracts typically omit arrangements for circumstances and situations that are of potential importance to the parties at a later stage. Drafting complete contracts, if possible at all, would be burdensome and costly. Default rules in contract law legislation help to lower transaction costs. Contracting parties may rely on such default rules without making the effort to negotiate a similar solution. The major sources for default rules are typical contract provisions used in legal practice. Such majoritarian default rules are used as a proxy for the assumption of what parties would have agreed upon if they had foreseen the need for an arrangement for a given situation.[76]

Default rules are nonetheless of a normative nature – even if inspired by neutral majoritarian default.[77] Contracts are negotiated 'in the shadow of default rules'.[78] The party who wishes to deviate from a default has the burden to argue against a statutory rule. Default rules may be used, e.g. in Germany, for challenging standard terms and conditions as deviations from a statutory standard.[79] Therefore, legislatures should not codify default rules which may lead to socially undesirable results. Moreover, default rules can be used proactively to 'nudge' the parties in the direction of what the legislature deems to be an individually or socially desirable choice.[80] With regard to contracts, such biased default rules have the effect

---

75 See already Friedrich C. von Savigny, *System des heutigen römischen Rechts, Bd. 1* (Veit 1840) 58; for the current law and economics theory of incomplete contracts see Cooter and Ulen (n. 63) 283–86; Shavell (n. 64) 299–301; Schäfer and Ott (n. 64) 431–34.

76 See Ian Ayres and Robert Gertner, 'Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules' (1989) 99 Yale Law Journal 87, 93; Gerhard Wagner, 'Zwingendes Privatrecht – Eine Analyse anhand des Vorschlags einer Richtlinie über Rechte der Verbraucher' (2010) Zeitschrift für europäisches Privatrecht 243, 256.

77 On the different theories of a normative function of default rules see Johannes Cziupka, *Dispositives Vertragsrecht* (Mohr Siebeck 2010) 90–136: '*gebietende Dimension des dispositiven Rechts*'.

78 Ayres and Gertner (n. 76) 95.

79 See Sec. 307 German Civil Code: '(1) Provisions in standard business terms are ineffective if, contrary to the requirement of good faith, they unreasonably disadvantage the other party to the contract with the user. ... (2) An unreasonable disadvantage is, in case of doubt, to be assumed to exist if a provision (1.) is not compatible with essential principles of the statutory provision from which it deviates ....'.

80 Cass Sunstein and Richard Thaler, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008) passim.

of, though are less intrusive than, means of market regulation. However, as means of market regulation they presuppose a political decision,[81] which in case of contracts and market regulation should be based on evidence of a market failure.[82]

### 2. *Building blocks from EU instruments, contract law principles and national law*

Based on this two-fold function of default contract rules, the first source for non-mandatory contractual rights of access and portability should be the majoritarian default approach. In which contract scenarios and under which circumstances would the parties to a B2B contract agree on access to and porting of data? Unfortunately, economic research does not provide much empirical evidence on this question.[83] Soft law instruments and the above-cited experience from national contract law may be used to suggest some first building blocks for possible default rules. However, such an approach can only be tentative and subject to further revision in the light of the development of business models and typical contractual arrangements in the market.

Starting with the European Commission's Communication 'Towards a common European data space' and the corresponding Staff working paper ('How to' guide), it is apparent that the Commission is on one side monitoring closely what is happening on the different markets, but on the other side is rather reluctant to come up with concrete suggestions for default rules. The Communication itself explains on a very abstract level what key principles should be respected in B2B contracts.[84] These principles can be used by courts and legislatures to develop more concrete default rules. However, they are far from giving direction for specific cases. The corresponding Staff working paper explores different business models for data-

81 More general Cass Sunstein, 'The ethics of nudging' (2015) 32 Yale Journal on Regulation 413, 415: 'It is true that all government action, including nudges, should face a burden of justification (and sometimes a heavy burden)'.

82 See Horst Eidenmüller, 'Liberaler Paternalismus' (2011) 66(17) JuristenZeitung 814, 819–20, who recommends welfarism as normative concept to justify nudges.

83 Only individual business models have been explored in the literature, e.g. European Commission Staff Working Document (n. 43) 8–18; see also Axel Metzger, 'Digitale Mobilität – Verträge über Nutzerdaten' (2019) Gewerblicher Rechtsschutz und Urheberrecht 129–136 on the automotive industry.

84 See at C.II.1., above, and European Commission, 'Towards a common European data space' (n. 43) 10.

sharing (open-data approach, data monetisation on a data marketplace, data exchange in a closed platform) and explains what parties should consider when agreeing on data access, e.g. what data is to be made available, who can access and (re-)use the data in question, what can the (re-)user do with the data, how to protect data, liability provisions, rights and obligations with regard to audits, duration of the contract, applicable law and dispute resolution mechanisms.[85] Yet the different aspects are drafted in the form of a checklist without concrete recommendations. Moreover, the issues addressed in the checklist are only of interest once the parties have reached consensus that one party should get access to data held by the other party. The key question, in which situations one party should have a (default) right to claim for access if not explicitly provided for in the contract, is not answered by the Staff working paper.

Looking into soft law principles developed by academic projects, two already mentioned general doctrines could be used for deriving access rights. First, it is commonly accepted, at least if one follows the Principles of European Contract Law, the Unidroit Principles or the Draft Common Frame of Reference (DCFR) that the parties to a contract must act in accordance with good faith and fair dealing.[86] One may well consider whether parties may infer from this principle certain information duties and claim for access to data, e.g. if the owner of an industry machine needs certain data for the maintenance of the machine – a case explicitly discussed as an illustration in the Comments to Article 5.1.2 Unidroit Principles.[87] Second, one may construe access rights as restitution claims in case of termination of a contract.[88] Also, one could consider – more specifically – applying the client's claim for the 'return of the thing processed' under the DCFR principles on service contracts.[89] These approaches, though drafted in a more general way, coincide to some degree with the non-mandatory rules of German contract law described above, according to which access rights can be justified in cases (1.) in which access to data is necessary for the stipulated use of the good or service, (2.) in which data has been transmitted to or deposited with a fiduciary or data processor

85 European Commission Staff Working Document (n. 43) 5–11.

86 See Art. 1:201 and 6:102 PECL; Arts 1.7. and 5.1.2. Unidroit Principles 2016; Art. I.1:103, II.9:101 DCFR. See also Arts 2 and 68 Common European Sales Law (CESL).

87 See Unidroit Principles 2016, 152.

88 See Arts 9:305–9:309 PECL; Arts 7.3.5.-7.3.7 UNIDROIT Principles 2016, Art. III.3:506–514 DCFR for the case of termination based on non-performance.

89 Art. IV.C.4:105(2) DCFR.

who processes the data on behalf of the client and (3.) in case of termination of a contract. It could be of main interest to gather experiences from other European jurisdictions to draw a more nuanced picture.

### *3. ALI–ELI Principles for a Data Economy*

The American Law Institute and the European Law Institute are currently working on a joint set of 'ALI-ELI Principles for a Data Economy – Data Rights and Transactions'. The project started in 2016.[90] The latest draft of black letter Principles and (tentative) comments is dated 22 May 2020.[91] The Principles contain non-mandatory rules for different kinds of data contracts in Principles 7 to 14. These contract law principles presuppose that the data controller has agreed to transfer or grant access to data or to permit the exploitation of data. The question discussed in this paper, whether a party can claim for access if the contract does not explicitly provide such a right, is not of interest in this part of the Principles.[92]

The ALI-ELI Principles do not stop at this point but also suggest, in Part III 'Rules and Principles Governing Data Rights', including a right to access or to port co-generated data. The access rights drafted so far are restricted to 'co-generated data'. Possible access rights for other data have not yet been drafted.[93] The notion of co-generated data is not defined with a hard and fast rule but depends on a set of factors, including whether the party interested in the data is the subject of the data, whether the data has

90 See <www.europeanlawinstitute.eu/projects-publications/current-projects-feasibility-studies-and-other-activities/current-projects/data-economy> accessed 31 August 2020.

91 The author of this contribution serves as a Member of the ELI Advisory Committee but has not been actively involved in the drafting of the Principles or comments. Direct citations from the draft principles are not permitted.

92 One provision resembles the problems discussed above: In a contract for the processing of data, where the processor undertakes to process data on behalf of the controller, the controller may ask for the processor to erase all data after the contract has been performed and the processed data has been provided to the controller. This reminds the reader of Art. IV.C.4:105(2) DCFR.

93 But the Principles already provide a section for 'Data Rights Beyond Co-Generation' in Principles 23–25. An additional special right of portability of reviews is suggested by Art. 7 ELI Model Rules on Online Platforms; see <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf> accessed 31 August 2020, and Busch and others, 'The ELI Model Rules on Online Platforms' (2020) 9(2) Journal of European Consumer and Market Law 61, 68.

been generated by the party's activity or use of a product or service or whether the data has been generated with a software or product produced by that party.[94] For co-generated data in that sense, the Principles suggest taking general factors into account when determining possible data rights, namely the share in the generation of the data, the weight of the legitimate interests of the parties, the imbalance of bargaining power and the public interest.[95] For access and porting rights, the Principles provide a non-exhaustive list of circumstances that may give ground for an access and porting right, especially if the data is necessary for the normal use, maintenance or resale of the product or service, for quality monitoring, for the understanding of the party's own operations, for the development of new products or services or for preventing a lock-in situation.[96]

The 'Rules and Principles Governing Data Rights' in Part III are not characterised as contract law but leave it to the applicable law to implement them in the appropriate legal framework.[97] This has the advantage of giving flexibility to courts, legislatures and other possible users of the principles. However, the mix of factors may also be seen as an impediment to their adoption since it may be difficult to use the suggested tests in a national legal framework which insists on the dividing line between the different areas of contract, competition and public law. The issue is not a merely doctrinal one but raises more fundamental concerns of policy. Is it, for example, reasonable to refer to a vague idea of imbalance of power if the threshold for a dominant position in the sense of Article 102 TFEU (or for one of the more recent concepts of competition law, e.g. from the current German reform projects)[98] is not met? One should keep in mind that the B2B contracts in question are not characterised by a structural imbalance like employer-employee, trader-consumer, landlord-tenant or publisher-author relationships.[99] Therefore courts and legislatures should be cautious to interfere with the freedom of contract in cases in which big and

94 See Principle 17(1) ALI-ELI Principles.
95 See Principle 18(1) ALI-ELI Principles.
96 See Principle 19(1) ALI-ELI Principles.
97 See Principle 15(2) ALI-ELI Principles.
98 See Sec. 18(3a) German Act Against Restraints of Competition; see also the Government Bill for a 10th revision of the German Act against Restraints of Competition (n. 67).
99 The argument of structural imbalance is used in German contract law to justify regulatory intervention in the mentioned areas; in this regard see the contributions of Karl Riesenhuber, 'Private Macht im Vertragsrecht – Langzeitverträge', Gralf-Peter Calliess, 'Private Macht und Verbraucherrecht' and Eva Kocher, 'Private Macht im Arbeitsrecht' and in Florian Möslein (ed.), *Private Macht* (Mohr

small companies conclude contracts, as long as those contracts are concluded on a market with functioning competition. The mere imbalance of power does not per se justify state intervention.[100] All European collections of soft law contract principles provide some sort of emergency exit for extreme cases with doctrines like excessive benefit, gross disparity, unfair exploitation.[101] One should not go beyond these doctrines – at least under contract law principles. The same line of argument may be applied to the criteria of prevention of lock-in situations. Are we sure that a lock-in situation with regard to maintenance services of digital products or services is always inefficient, even if a smaller competitor on the market for the product protects a specifically safe and therefore costly environment for its customers? This may be the unique selling point of such a smaller competitor in a market with other more dominant actors. Or as final point, do we really want courts and legislatures to interfere with the freedom of contract based on a broad notion of public interest? Should courts engage in industry policy or save jobs or the local businesses? For the purpose of this paper, which is focused on contract law, it must suffice to say that any intervention affecting freedom of contract should be based on clear evidence of a market failure. It is admitted that the ALI-ELI Principles give total flexibility to legislatures and courts to pick and choose the factors that may fit into the respective regulatory framework and set aside the other listed criteria. However, one should not be surprised if in the end the factors are also used for the justification of misguided and inefficient interventions.

The critical stance taken here on some of the factors suggested by the ALI-ELI Principles reflects in more specific terms what has been said earlier about the function of default contract rules. Either they codify majori-

---

Siebeck 2016) 193, 213, 241 respectively. From the older literature see Lorenz Fastrich, *Richterliche Inhaltskontrolle im Privatrecht* (C.H. Beck 1992) 159–201, 216–21; Günther Hönn, *Kompensation gestörter Vertragsparität* (C.H. Beck 1982) 153–160.

100 See in this regard the apparent caution of leading law and economics handbooks, e.g. Richard A. Posner, *Economic Analysis of Law*, (9th edn, Wolters Kluwer Law & Business 2014) 127–28; Schäfer and Ott (n. 64) 487–90. See also Roland Kirstein and Matthias Peiss, 'Quantitative Machtkonzepte in der Ökonomik' in Florian Möslein (ed.), *Private Macht* (Mohr Siebeck 2016) 91–117. See also the contributions of Carsten Herresthal, 'Private Macht im Vertragsrecht – Austauschverträge' Friedemann Kainer, 'Private Macht im Kapitalmarktrecht' and Heike Schweitzer, 'Wettbewerbsrecht und das Problem privater Macht' in Möslein (ibid.) 145, 423, 447 respectively.

101 In this regard see Art. 4:109 PECL; Art. 3.2.7 Unidroit Principles; Art. II.7:207 DCFR; see also Art. 51 CESL.

tarian default rules to help parties with incomplete contracts or they pursue enforcement of policy choices through the, compared to mandatory rules, less intrusive mechanism of defaults. Some of the factors listed by the ALI-ELI Principles may help to identify majoritarian defaults, e.g. the share of the contracting parties in the generation of the data, the necessity of the data for the normal use, maintenance or resale of the product or service, or its necessity for quality monitoring or for the understanding of the party's own operations. However, it is apparent that some of the factors suggested by the ALI-ELI Principles belong to this second type of default rules, e.g. the imbalance of bargaining power, the public interest, the necessity of data for the development of new products or services or for preventing a lock-in situation. This begs the question of the justification of policy choices behind those factors and how well they serve the purpose of increasing social welfare.

### *D. Conclusion*

This chapter started with the question whether a party under a contract is obliged to grant the other party access to data it has collected. The answer given in this chapter based on an analysis of European and German contract law depends on whether the claimant is a consumer or a business user.

For consumers, Article 16(4) DCSD now stipulates for a right of access and portability with regard to non-personal data, which was provided or created by the consumer. However, this right is superseded to a large extent by Article 20 GDPR, which takes priority for personal data. Moreover, Article 16(4) DCSD is not applicable to access to data stored in devices with embedded software on which the new Directive on the sale of goods is applicable. Additional limitations of the scope of Article 16(4) DCSD arise from the fact that the provision is only applicable in the case of termination of the contract resulting from the failure to supply or a lack of conformity. The scope of application of Article 16(4) DCSD will therefore be rather limited. It will be of interest in the coming months to see how EU Member States deal with this limited scope and whether they go beyond this minimalist approach – if not in the implementing legislation then by case law in the years to come. Arguments for a careful extension could be taken from the principles of general contract law described in this paper, which are applicable both to B2B and B2C contracts. In this regard, it has been shown that national contract law may grant specific access rights based on the principle of good faith or as implied terms, e.g. with regard

to cloud services that store data on behalf of the client, for data necessary for the performance of a purchased good or in cases of termination of contracts. In regard to these general contract law doctrines, Article 16(4) DCSD does not fall into a vacuum. The DCSD could be used as a focal point for further development of contractual access rights for consumers, even though the scope of application of Article 16(4) may remain limited in the near future.

For B2B contracts, it has been shown that neither European nor national contract law provides for mandatory access and porting rights until now. Against this backdrop, the paper has argued that there is no legal basis or economic evidence justifying the introduction of general contractual access or porting rights. Competition law may call for additional access rights effected by contractual means if markets are not functioning well. Information asymmetries may require transparency on the existence or non-existence of collected data and contractual data access rights, as now partially provided for in the Fairness and transparency Regulation. But legislatures should be cautious to adopt broad contractual access rights beyond these sector-specific instruments with reference to concepts like imbalance of bargaining power, prevention of lock-in or the general public interest. Yet, this cautious approach should not prevent European or national legislatures to enact default rules on data access and portability applicable to B2B contracts, which can be derogated from by agreement. Such rules should reflect the majoritarian defaults used – or presumably used – in the market. In this regard, the above-mentioned experience from national contract law could be helpful. Also, the principles developed by the EU Commission in its recent Communications and some of the factors put forward by the ALI-ELI Principles for a Data Economy can play a role. Also, it will be highly interesting to see whether Article 16(4) DCSD triggers a change of the business practice of traders also for professional users or if it changes at least the courts' perceptions of what reasonable parties would have agreed upon if they had foreseen a later claim for access to data. But these default rules should be based on actual or presumed majoritarian defaults. Such an approach could help to facilitate data sharing as envisioned by the recent 'European strategy for data'.[102] Going beyond this line – with default rules as 'nudges' for horizontal B2B access rights – would require evidence for a market failure beyond specific sectors.

102 COM(2020) 66 final, 13.