IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES No. 23-01

THE DATA ACT PROPOSAL

Literature Review and Critical Analysis

Moritz Hennemann / Benedikt Karsten / Marie Wienroeder / Gregor Lienemann / Gordian Ebner (Eds.)

by

Moritz Hennemann / Gordian Ebner / Benedikt Karsten

Part I (Art. 1-13, 35)

Version 1.0

January 2023

Place of Publication

University of Passau IRDG
Innstraße 39
94032 Passau
https://www.jura.uni-passau.de/irdg/

Editors

Moritz Hennemann is a Full University Professor, holding the Chair of European and International Information Law, University of Passau Law Faculty since 2020. His research focuses on private law, business law, data law, media law, and information law, including from a comparative perspective. He holds degrees in law from the Universities of Heidelberg (2009), Oxford (M.Jur., 2011), and Freiburg (Dr. jur., 2011). He was a postdoctoral researcher at the University of Freiburg (Habilitation, 2019), a visiting researcher at Harvard Law School and an affiliate to the Berkman Klein Center for Internet & Society, Harvard Law School.

Benedikt Karsten is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2022. His research focuses on data law. He holds a degree in law from the University of Passau (2020) and is a fully qualified lawyer (Ass. jur., 2022).

Marie Wienroeder is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2022. Her research focuses on data law. She holds a degree in law from the University of Passau (2022).

Gregor Lienemann is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2021. His research focuses on data portability and on the intersection of data protection and competition law, including from a comparative perspective. He holds degrees in law from the Universities of Munich (2020) and Reading (LL.M., 2021).

Gordian Ebner is an academic research assistant at the Chair of European and International Information Law, University of Passau Law Faculty since 2020. His research focuses on data protection law, especially data-related information duties. He holds degrees in law from the University of Passau (2020 and Dr. jur., 2022).

https://www.jura.uni-passau.de/hennemann/

Abstract

This three-part publication critically evaluates the Commission's Proposal for a Data Act. It provides an in-depth analysis of the Proposal. The concept of the Act is critically examined and the instruments proposed are thoroughly evaluated and put into context. The existing literature

on the Act is mapped and mirrored. Proposals for amendments to the Act are considered. This publication aims to contribute to the on-going debate about and the legislative process of the Act.

Cite as

Hennemann, M. / Ebner, G. / Karsten, B. (2023). Part I (Art. 1-13, 35), in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (Eds.). The Data Act Proposal – Literature Review and Critical Analysis. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-01*.

All parts of this three-part publication on the Data Act Proposal are available at https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Data Act, Data Governance, EU, Data Strategy, Access Rights, Unfair Terms, SMEs, Cloud Services, Data Transfers, Interoperability, Data Portability, Transparency

Foreword by the Editors

Dear Fellow Reader,

Since February 2022, the wider public and the Data Law community in particular has had the chance to have a look at the Commission's Proposal for a Data Act. From then on, manifold discussions have begun – including within the European Parliament. Up to this date, we have seen three proposals by the Council's presidency to amend the Commission's proposal – and at least one more is said to come. To assist this process, we have – as a first step – published a Data Act – Article-by-Article Synopsis (systemizing provisions, recitals, and definitions) in March 2022.

This Literature Review and Critical Analysis of the Data Act Proposal – as a second step – provides an (more) in-depth analysis of the Proposal. It is presented in three parts / documents (all accessible here) and also builds upon first contributions to the debate by Hennemann, M. / Steinrötter, B., Data Act – Fundament des neuen EU-Datenwirtschaftsrecht?, *Neue Juristische Wochenschrift (NJW)* 2022 (21), 1481-1486 and Ebner, G., Information Overload 2.0? – Die Informationspflichten gemäß Art. 3 Abs. 2 Data Act-Entwurf, *Zeitschrift für Datenschutz (ZD)* 2022 (7), 364-369; Karsten, B. / Wienroeder, M., Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie, *Recht Automobil Wirtschaft (RAW)* 2022, 99-105; Hennemann, M., Datenrealpolitik – Datenökosysteme, Datenrecht, Datendiplomatie (2022) *University of Passau IRDG Research Paper Series No. 22-18*).

The concept of the Data Act is critically examined and the instruments proposed are evaluated and put into context. Especially, the study also considers the on-going legislative debate within the European Parliament and especially depictures the amendment proposals of the Council Presidency. In addition, reference is not only given to the growing literature on the Data Act proposal (there is very much…), but the current state of discussions is mapped and mirrored – and, where appropriate – this Literature Review and Critical Analysis takes a stand on existing proposals for amendments to the Act and / or proposes further amendments to be considered.

We have especially looked at those parts of the Act (especially Chapter VI on "Switching between Data Processing Services") which have not got the same attention than the omnipresent access rules of Art. 4 et seq. This Part I includes an Executive Summary.

This Literature Review and Critical Analysis will be amended in due course – it is *work-in-progress* and just an Open Access-Version 1.0 – and is meant to be published in a revised version after the finalisation of the Data Act (whenever that might be…).

We are more than happy to hear your thoughts about this Literature Review and Critical Analysis in general and about what we have missed – and warmly welcome recommendations in order to close gaps and to correct us! Please drop us an e-mail to moritz.hennemann@uni-passau.de.

We like to thank the entire team at the chair of European and International Information and Data Law and at the Research Centre for Law and Digitalisation (FREDI) for their extremely valuable support in the drafting process and for taking the burden of formatting the documents.

Sincerely yours,
Moritz Hennemann, Benedikt Karsten, Marie Wienroeder,
Gregor Lienemann & Gordian Ebner

Version 1.0

Contents

I. Executive Summary (Part I-III)

1. The Data Act proposal is a **push into the right direction**. Its focus on non-personal and personal data use and data usability deserves support. Its **actual design** is, however, **not in every way convincing**, and **requires structural amendments** and **amendments in detail**.

2. The Data Act is first and foremost seeking to enhance **compulsory data sharing** with regard to different actors and in commercial and non-commercial data ecosystems.

3. The Act is introducing **statutory data access rights** in the favour of users of IoT-products (Art. 4 et seq.) as well as public authorities in specific cases (Art. 14 et seq.). The Data Act does not introduce general access rights. In the context of IoT-products, the access rights are linked to the data 'generated by the use' and are dependent on a **user's request** to grant direct access to himself and / or to a **third-party recipient**. There are no access rights to the benefit of the public and / or the market participants / the economy in general.

4. The data access is combined with underlying contracts / agreements enabling data use. The Data Act is fostering contractual agreements between (nearly) all relevant parties (data use agreement, data access contract (on FRAND terms), non-disclosure-agreements (NDAs). The Data Act is supporting a process of "**contractualisation" of Data Law**. It is against this background highly and rightly criticized that the Data Act does **not stipulate** any **conflicts of law-rules**.

5. Despite this process of "contractualisation", the Data Act does not provide (beside Art. 13) any specific rules in detail for the central **data use agreement according to Art. 4(6)**. Generally, rules on **standard terms control** are rather **limited in substance** and only applicable for contracts with micro, small, or medium-sized enterprises (Art. 13). The Data Act does therefore also **not** contain **rules for data contracts vis-à-vis customers** (and leaves this to the member states). On the basis of Art. 34, however, model contract clauses shall be developed.

6. The data access is restricted by different rules – especially with regard to a data use with regard to **competing products** / **competing markets** (Art. 4(4), 5(5), 6(2)(e)) as well as with regard to **gatekeepers** according to the DMA (which are considered to be illegitimate as third-party recipients, Art. 5(2), 6(2)(d)).

7. It is **highly debated** whether and to what extent the data access regime sets – from a **Law & Economics** perspective – functionally calibrated, sensible, and thought-through parameters and incentives. It is *inter alia* debated which **kind of data** shall be made accessible, especially with regard to 'raw data', 'prepared data', 'derived', 'inferred', and / or 'aggregated' data. It is discussed whether the **user activation** (the Data Act relies on) will work in practise. It is considered whether **sectoral approaches** shall be favoured in opposition of the one size fits all-framework of the Data Act. Furthermore, it is questioned whether the **exclusion of gatekeepers** as third-party recipients is serving the innovation and the common wealth. Finally, the (setting of) **FRAND conditions** (Art. 8(1)) is confronted with doubt regarding practicability.

8. From a mostly, but not only, doctrinal point of view it is heavily debated whether and to what extend the data access regime introduces and / or paves the way for some type of **'absolute' / 'IP-like' right regarding non-personal data**. This debate has to be seen against the background that on the basis of the current law non-personal data (if one has access and notwithstanding trade secret law) can be used freely and without some form of consent and / or agreement by the 'producer'. The regulation proposed by the Data Act can be understood as to manifest the ***technical-factual 'rule'* of the data holder** who might have to grant access. To the same end, others do underline the co-generating of data by data holder and user. Some commentators connect such a **co-generation** with the idea of a **'co-property'** (*Miteigentum*) leading towards a general 'right' of both the data holder and the user to use the respective non-personal data. At least, from our point of view, the need for a **data use agreement with the user according to Art. 4(6)** does even point to an **'attribution'** (without constituting an absolute right) of the respective data to the user. It is another question that right now whether and in which setting users will actually negotiate and / or value this agreement in practise.

9. The Act also introduces new **access rights for public sector bodies**. In contrast to Chapter II, these access rights are independent from a user. meaning that the public sector body can request data directly from the data holder. The public sector body has to demonstrate an exceptional need to access data. Micro and small enterprises are excluded from the obligation to make data available (Art. 14(2)). This exemption is not fully convincing as the burden on micro and small enterprises could also be addressed through compensation. Furthermore, the current proposal also **fails to differentiate between non-personal and personal data.** While even more extensive access rights regarding non-personal data could be justified, the provisions of Art. 14 and 15(c) seem to be too broad and too unspecific to justify the processing of personal data.

10. The Data Act seeks to regulate providers of data processing services (i.e. **cloud and edge computing** businesses). The proposed rules raise doubts with regard to technical feasibility and economic incentives. Commentators have called into question the technical feasibility of, in particular, the withdrawal of switching charges (Art. 25) and the mandate for **functional equivalence** of service at the destination (Art. 23(1)(d), read jointly with Art. 26(1)). Likewise, the fact that differently sized (SaaS) cloud providers all have to meet the same requirements has drawn criticism.

11. With **smart contracts** (or more precisely, the distributed ledger technology) being regarded as a viable avenue for data sharing, Art.30 aims for standardisation of these self-executing protocols through key security requirements.

12. The rule on **international transfer of non-personal data** (Art. 27) comes along with the same uncertainties as the parallel norm in Art. 31 Data Governance Act. In particular and without prejudice to Art. 27(2) and (3), Art. 27(1) shall not be read in a way that providers of data processing services must seek to prevent any transfer to or access from a non-EU country in conflict with Union law or laws of the Member States. A respective requirement is not very burdensome, but might lead providers

to refrain from international transfers at all. Rather, Art. 27(1) should target rules specifically prohibiting data transfer to and access from third countries.

13. From a legal point of view, it is highly unsatisfying that the Data Act for all parts **does not solve** and / or complicates the relationship to and its **interplay with data protection law** / the **General Data Protection Regulation** (GDPR). Recent proposals by the Council Presidency underlining that the Art. 4 et seq. are generally not being regarded as legal ground according to Art. 6(1)(c) GDPR are **fundamentally opposing the general aim** of the Data Act to enhance and foster data sharing and data use.

14. Additionally, and even more surprising, it is hard to comprehend that the Data Act **does not substantially tackle** the relationship to and its **interplay with the Data Governance Act** (DGA). Specific rules are missing and no incentives are set (for example to the benefit data intermediaries). As data intermediaries do – potentially fulfil a central function in order to enable data exchanges / data contracts (*inter alia* between users and third party recipients), the gap **fundamentally opposes the general aim** of the Data Act to enhance and foster data sharing and data use.

15. The Data Act increases the **regulatory complexity** for the data economy. With regard to the aim of boosting data access and fairness in data markets that is evitable – and it is to be welcomed that the Data Act does introduce – however, not for all parts of the Act – some specific rules to the benefit of and some exceptions regarding **micro, small, or medium-sized enterprises**.

16. The Data Act – and especially its access rights – will be **complemented by sector-specific EU legislation** (in particular by **European Data Spaces** legislation). It is, however, entirely clear whether and to what extent the Data Act leaves room for **Member State legislation** in specific sectors – as it is *inter alia* planned by the German Federal Government.

17. Finally, the Data Act is **rather vague** on the central question whether and to what extent a **monetarisation** of personal and – especially – non-personal data shall be possible. Different follow-on rules of the access right (e.g., Art. 4(4), 5(5), 6(2)(c) and (e)) limit – next to data protection law – a full monetarisation. At least slightly, Art. 4(6) and Art. 6(2)(f) might be interpreted to point to the **user** as being the prime actor to monetarise.

18. With the Data Act and the Data Governance Act, the EU has again been a ***first mover*** in the **'market of regulatory ideas'**. With regard to the **severe criticism** from an Economics angle as well as with regard to the missing interplay between the two Acts and between the Acts and the GDPR, it is at least **doubtful** that the Data Act (and the Data Governance Act) will be able to **unleash its full potential**. It is, for example, rather foreseeable that unchanged data protection restrictions will serve as a (maybe welcomed) barrier for data holders to grant access.

II. Introduction

On February 23 2022, the Commission unveiled its long-awaited Proposal for a Data Act[1] – and the debate has taken up speed since then.[2] The Proposal introduces – in the form of a regulation[3] – sweeping mandates to grant access to datasets to the benefit of both private and public entities, and accentuates a contractual angle into regulating the exchange and shared use of data in the digital economy. It strives for general accessibility, interoperability, and portability of data with technical safeguards and firm limitations for re-use in the data lifecycle.

---

[1] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access and use of data (Data Act)' COM(2022) 68 final.

[2] Contributions to the debate include, but are by no means limited to the following publications: Bitkom, 'Bitkom Position Paper EU Data Act Proposal' (19 April 2022); Bomhard, D. / Merkle, M., Der Entwurf des Data Act – Neue Spielregeln für die Data Economy, *RDi* 2022, 168; BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022; Brauneck, J., Zur Vereinbarkeit des Data Act-Entwurfes mit dem Europäischen Wettbewerbsrecht, *WRP* 2022, 954-961; Derclaye, E. / Husovec, M., Why the sui generis database clause in the Data Act is counter-productive and how to improve it? (8 March 2022, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052390); Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), White Paper on the Data Acto Proposal, *CiTiP Working Paper* 2022; Ebner, G., Information Overload 2.0? – Die Informationspflichten gemäß Art. 3 Abs. 2 Data Act-Entwurf, *ZD* 2022, 364; Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022; Gerpott, T., Vorschlag für ein europäisches Datengesetz Überblick und Analyse der Vorgaben für vernetzte Produkte, *CR* 2022, 271; Graef, I. / Husovec, M., Seven Things to Improve in the Data Act (7 March 2022, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793); Hartmann, B. / McGuire, M. R. / Schulte-Nölke, H., Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act): Rechtliche Rahmenbedingungen für die Vertragsgestaltung, *RDi* 2023, 49-59; Hennemann, M. / Steinrötter, B., Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, *NJW* 2022, 1481; Heinzke, P., Data Act: Auf dem Weg zur europäischen Datenwirtschaft, *BB* 2023, 201-209; Hilgendorf, E./Vogel, P., Datenrecht im Umbruch. Aktuelle Herausforderungen von Datenschutz und Datenwirtschaft in Europa, *JZ* 2022, 380; Karsten, B. / Wienroeder, M., Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie, *Recht Automobil Wirtschaft (RAW)* 2022, 99-105; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022; Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107; Klink-Straub, J. / Straub, T., Data Act als Rahmen für die gemeinsame Datennutzung *ZD-Aktuell* 2022, 01076; Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022; Mell, P. / Grance, T., The NIST Definition of Cloud Computing, *NIST Special Publication* 800-145, 2011; Metzger, A. / Schweitzer, H., Shaping Markets: A Critical Evaluation of the Draft Data Act, *ZEuP* 2023, 42; Max Planck Institute for Innovation and Competition, Position Statement, 2022; MyData Global response of the Data Act, 2022; Perarnaud, C. / Fanni, R., The EU Data Act – Towards a new European data revolution?, 2022; Picht, Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022; Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022; Podszun, R. / Pfeifer C., Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, *GRUR* 2022, 953; Schaller, T. / Zurawski, P., Staatlicher Kompetenzaufwuchs im Data-Act-Entwurf, *ZD-Aktuell* 2022, 01169; Schneidereit, P., Auswirkungen des Data Act auf innovative datengetriebene Geschäftsmodelle in der Medizintechnik: Analyse wesentlicher Auswirkungen auf die Praxis, *CR* 2023, 9-14; Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022; Specht-Riemenschneider, L., Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?, *ZRP* 2022, 137; Specht-Riemenschneider, L., Der Entwurf des Data Act, *MMR* 2022, 809; Staudenmeyer, D., Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz, *EuZW* 2022, 596; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022; vbw, Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022; Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022.

[3] Supporting this approach Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 72.

In light of increasing legislative complexity (not only) emanating from the Commission, a systematic overview – and update – on the Data Act proposal hopefully contributes to a better understanding how this jigsaw piece fits with the broader strategic outlook and concomitant statutory instruments (e.g., Regulation (EU) 2022/868 (Data Governance Act)[4] and Regulation (EU) 2022/1925 (Digital Markets Act)[5]). Against this background, this Literature Review and Critical Analysis engages with the Data Act in detail as well as engages with the cumbersome literature on the Data Act since its publication. Especially, the study also considers the on-going legislative debate within the European Parliament[6] and the different compromise texts of / proposals for amendment by Council Presidency[7] (in part also mirroring respective proposals form the Parliament's Committees Draft Reports).

1. General Setting and Goals

The challenges to be tackled by and the goals pursed with the Data Act are diverse.[8] The Act is mainly pointing to the unwillingness to share data by those who have access and is targeted at fostering data sharing, especially to boost innovation in aftermarkets.[9] Although the most prominent part of the Act is directed at *internet of things*-products (Art. 4 et seq.), the Act is not primarily concerned with competition on these primary markets.[10]

Rec. 1 highlights:

> "In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The proliferation in products connected to the Internet of Things in particular has increased the volume and potential value of data for consumers, businesses and society. High quality and interoperable data from different domains

[4] Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance.

[5] Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector.

[6] Parliament Committee on Industry, Research and Energy, 'Draft report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 14 September 2022; Parliament Committee on the Internal Market and Consumer Protection, 'Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 4 October 2022; Parliament Committee on Legal Affairs, 'Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', 6 October 2022; Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on Harmonised rules on fair access to and use of data (Data Act)', 19 October 2022.

[7] Council Presidency, 'Note on the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) - Second Presidency compromise text (Chapters I-V)', 21 October 2022; Council Presidency, 'Note on the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) - Second Presidency compromise text (Chapters VI-XI)', 3 November 2022; Council Presidency, 'Note on the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) – Third Presidency compromise text', 8 December 2022.

[8] Cf. also Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 5 et seq.

[9] See Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 5 who has strong doubts whether the Act's design will fulfil this goal (cf. p. 19).

[10] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 6.

> increase competitiveness and innovation and ensure sustainable economic growth. The same dataset may potentially be used and reused for a variety of purposes and to an unlimited degree, without any loss in its quality or quantity.

On this basis, Rec. 6 sets the general regulatory setting of the Act:

> "Data generation is the result of the actions of at least two actors, the designer or manufacturer of a product and the user of that product. It gives rise to questions of fairness in the digital economy, because the data recorded by such products or related services are an important input for aftermarket, ancillary and other services."

Rec. 2 outlines the main "[b]arriers to data sharing" the Act is willing to tackle:

- "lack of incentives for data holders to enter voluntarily into data sharing agreements"
- "uncertainty about rights and obligations in relation to data"
- "costs of contracting and implementing technical interfaces"
- "the high level of fragmentation of information in data silos"
- "poor metadata management"
- "the absence of standards for semantic and technical interoperability"
- "bottlenecks impeding data access"
- "lack of common data sharing practices"
- "abuse of contractual imbalances with regards to data access and use"

Rec. 4 underlines that the Act "respond[s] to the needs of the digital economy and (…) remove[s] barriers to a well-functioning internal market for data" (the latter is inter alia underlined by the rules on switching between data processing services according to Art. 23-26).

The Draft Report of the Committee on Industry, Research and Energy (ITRE) additionally highlights the need "avoid the fragmentation of the internal market that could emerge from national legislation".[11]

The Data Act seeks to promote innovation by access and to incentivise data production. Rec. 28 elaborates in this regard:

> "The aim of this Regulation should accordingly be understood as to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services. At the same time, it aims to avoid undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product."

[11] ITRE PE732.704, p. 6.

Rec. 28 additionally points to – also with regard to the protection of trade secrets – that "[i]t is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product."[12]

JURI is proposing to include the dimension "data literacy" to the Act by proposing a new Art. 3a on this topic.[13]

2. From A Reaction to Market Failures to Market Design and Market Infrastructure

The various aforementioned drivers in favour of the Data Act laid down by the Commission underline a general tendency in European Data Law. First, the different legislative proposals do not and do not want to fit neatly into a specific field of law. Central questions, e. g., the nature of specific rights, remain open. They often combine different, not always directly connected, fields aspects of data governance. This is also and especially true for the Data Governance Act which tackles only selected fields like public sector information, data intermediation services, and data altruism – and does not strive to set coherent rules.

Second and most importantly, it has already become clear from the Data Governance Act that the Commission and / or the legislator do not only strive to counter perceived or actual market failures – as a traditional Economics perspective would advise to do.[14] Rather, the Acts must be described as a form of *market design law* or *market infrastructure law*.[15] The different Acts are not only meant as setting boundaries for specific activities – neatly underlined by the fact that the Acts pursue a horizontal approach and are not only e. g. applicable to a specific sector[16] or to dominant undertakings[17] (the Data Act is consequently described as a "horizontal fundamental piece of regulation for all sectors"[18]). Therefore, the Acts are rather directed at establishing and boosting distinct market actors (e. g., data intermediation services) as well as shaping existing and in part creating new markets.[19] Contrary to traditional doctrine, but in line

[12] Cf. also the proposal of a Rec. 28a regarding trade secrets by Council Presidency 2022/0047(COD) – 13342/22, p. 15; cf. also ITRE PE732.704, p. 16.

[13] JURI PE736.696, pp. 28 et seq.

[14] See Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 77. Cf. in detail on the economic justification of the Act Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 15 et seq. n. 32 et seq.

[15] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 78; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 117; Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (50). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 17 et seq. n. 39.

[16] Demanding respective complementary sectoral rules, Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 6; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 3 n. 3.

[17] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 211, 213; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 15 et seq. n. 33.

[18] Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (955): "horizontales Grundlagenwerk für alle Sektoren" (translation by authors).

[19] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 116.

with modern Economics approaches of market shaping (*Mazzcato*)[20], the legislative instruments are to be understood – and might be regarded as justified – as being targeted at *transformation*.[21]

Finally, however and in contrary, this is not to say that the Act – next to its *market design* approach – does actually address all market failures in question.[22]

3. "Contractualisation" of Data (Economy) Law

The Acts strives to "to realise the important economic benefits of data as a non-rival good for the economy and society" and supports "a general approach to assigning access and usage rights on data" (Rec. 6). Such an approach is regarded as superior to the award of "exclusive rights of access and use" (Rec. 6).

Accordingly – and referring to the broad debate on "data property" or absolute rights to data – Rec. 5 states that the Act "should not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service."[23] (the Council Presidency, however, connected the aforementioned reference in her third compromise text with a legal basis according to Art. 6(1)(c) and (3) Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR))[24])[25].

The act seeks to takes "as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services." (cf., however, the discussion about Art. 4(6) below).[26]

On that basis, the Data Act is driven by a *contractualisation* of the relevant relationships between data holder, data user, and data recipient.[27] As a default, the Act refers to a scenario where a product or service is used on a contractual basis and data is generated in the context of this very contract[28] (however, the data holder (being obliged to grant access) and the contractual partner of the user, however, might be two different persons (cf. also Art. 3(2)(e)). Data access is generally combined with underlying (bilateral) contracts / agreements enabling data use.[29] The Act is consequently fostering contractual agreements between (nearly) all relevant parties

---

[20] Mazzucato, M., A collective response to our global challenges: a common good and market-shaping approach (UCL Institute for Innovation and Public Purpose Working Paper 2023-01), pp. 9 et seq.

[21] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 116.

[22] See in detail Kerber, W.,Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 2.

[23] Similar Rec. 24: "However, this Regulation (…) should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service."

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[25] Council Presidency 2022/0047(COD) – 15035/22, p. 8.

[26] Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 16 n. 34.

[27] In detail Staudenmeyer, D., *EuZW* 2022, 596 (596 et seq.). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 27 n. 68; Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 74.

[28] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[29] Staudenmeyer, D., *EuZW* 2022, 596 (596).

(data use agreement, data access contract (on FRAND terms), non-disclosure-agreements (NDAs).[30] *Leistner* and *Antoine* correctly point to a "contractual design and enforcement in larger, multipolar networks" (and the missing rules of the Data Act in this regard).[31]

Despite this process of *contractualisation*, the Data Act does not provide (beside Art. 13) specific contract law rules in detail, e.g., for the central data use agreement according to Art. 4(6).[32]

Furthermore, the proposed rules on standard terms control are rather limited in substance and only applicable for contracts with micro, small, or medium-sized enterprises (Art. 13). The Data Act does therefore also not contain rules for data contracts vis-à-vis customers (and leaves this to the member states). On the basis of Art. 34, however, model contract clauses shall be developed. Finally, the Data Act is generally rather silent on mechanisms of private enforcement and / or contractual consequences of violations of the Act's obligations.[33]

Generally, the Act underlines that Data (Economy) Law is driven by Contract Law. Rec. 5 underlines respectively that "[p]rivate law rules are key in the overall framework of data sharing" and that "[t]herefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances" (especially with respect to micro, small or medium-sized enterprises). Accordingly, the Data Act does not introduce a (direct) right to access of a competitor / third party that is fully independent of a user or its contractual relationship(s) (cf. also Art. 4(6) Sentence 1).[34]

4. User Activation

The Data Act heavily relies on an activation of the user. Thereby the access regime of the Data Act adopts a similar approach as the right to data portability according to Art. 20 GDPR does (which is faced with many obstacles and is said to be ineffective and / or under-used in practise).

The user has – at least formally[35] – a central role in the Data Act framework.[36] A processing of non-personal data by the data holder is only possible on the basis of a contractual agreement with the user (Art. 4(6)). Only the user may request access to the data generated by the user's use of an IoT-product – in favour of himself / herself (Art. 4(1)) or to the benefit of a third party

---

[30] Staudenmeyer, D., *EuZW* 2022, 596 (596 et seq.).

[31] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 75.

[32] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 74.

[33] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 13, 74; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 4 et seq. n. 6 and 8. This is also criticized from an Economics perspective, cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 10.

[34] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[35] Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956). Cf. for doubts re the actual position of the user below IV. 3. and 4. As well as Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 2.

[36] Cf. for the respective discussion Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 80, 98.

(Art. 5(1)). The user is thereby free to use both rights cumulatively.[37] Any access of a third party is dependent on the user (Art. 5(1)) – and consequently on a respective contractual agreement with the user. The third party will practically have to set financial incentives in order to 'activate' the user respectively.[38] Furthermore, the third party may not hinder the user to grant access to further third parties (Art. 6(2)(f)).

It is therefore heavily discussed whether this activation will actually on will work in practise.[39]

5. Monetarisation of Data?

Furthermore, the Data Act is rather vague on the central question whether and to what extent a monetarisation of personal and – especially – non-personal data shall be possible.[40] Although the general purpose of the Act, the different access rights stipulated by the Act as well as a well-understood interplay with data intermediation services generally – and rightly – foster the general possibility.

Different follow-on rules of the access right (e.g., Art. 4(4), 5(5), 6(2)(c) and (e)), however, limit – next to data protection law – a full monetarisation. At least slightly, Art. 4(6) and Art. 6(2)(f) might be interpreted to point to the user as being the prime actor to monetarise.[41]

The LIBE Committee explicitly goes the opposite way by proposing a new Art. 6(2)(fa) which forbids to:

> "commercially incentivise the data subject by providing monetary or other compensation for making personal data available."[42]

[37] Specht-Riemenschneider, L., *MMR* 2022, 809 (816).

[38] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 15.

[39] Cf. e. g., Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 81, 97; Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956).

[40] In detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 7 et seq. n. 14 et seq.

[41] See also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 18 n. 42. Cf. for doubts from an Economics perspective Cf. in this regard Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21.

[42] LIBE, PE737.389, p. 44.

III. Regulatory Scope and Intentions (Art. 1-2, Art. 35)

Chapter I ('General Provisions'; Art. 1-2) frames the Proposal in terms of scope and terminology, defining key concepts and the complementary relationship with applicable legislation on data protection, electronic communications, and criminal matters. It is therefore best contrasted with Chapter X ('*Sui Generis* Right under Directive 1996/9/EC'; Art. 35), which curbs protection granted to databases by way of a *sui generis* right within the ambit of the Proposal.

1. Scope (Art. 1 paras. 1 and 2)

Material Scope

According to Art. 1(1) the Data Act is focussed on data in the sphere of data holders, that is to say data generated by the use of a product or related service. If not explicitly stated otherwise, data refers to personal and non-personal data.[43] This data shall be made (better) available – according to specific requirements – to the user, third party data recipients, and / or public sector bodies or Union institutions, agencies or bodies. In this context, Rec. 5 points to the fact that the access shall be "in a timely manner" and that the user is generally free to pass data to data recipients of their choice. In substance, the Data Act provides for different, but intertwined instruments.[44] Rec. 5 summarises:

> "It imposes the obligation on the data holder to make data available to users and third parties nominated by the users in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and in a transparent manner. (…) This Regulation also ensures that data holders make available to public sector bodies of the Member States and to Union institutions, agencies or bodies, where there is an exceptional need, the data that are necessary for the performance of tasks carried out in the public interest. In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union."

The Council Presidency tries to clarify the material scope by proposing a new Art. 1(1a).[45] Art. 1(1a) explicitly states the scope of application for each chapter of the Data Act.

The Council Presidency further adds a new Art. 1(2a) (deleting Art. 7(2) at the same time): "Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants insofar as they interact with a product or related service."[46]

Personal Scope

Following this setting, Art. 1(2) defines the personal scope of the Act. The Regulation applies to

---

[43] This approach is mostly welcomed, cf. e. g., Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 9.

[44] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[45] Council Presidency 2022/0047(COD) – 13342/22, p. 35.

[46] Council Presidency 2022/0047(COD) – 15035/22, p. 39.

> (a) manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services;
>
> (b) data holders that make data available to data recipients in the Union;
>
> (c) data recipients in the Union to whom data are made available;
>
> (d) public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request;
>
> (e) providers of data processing services offering such services to customers in the Union.[47]

It remains unclear whether there is a difference between "placed on the market" (lit. a) and "offering such services".[48]

Territorial Scope

It is important to note that Art. 1(2) combines the personal and territorial scope of the Data Act.[49] With references to products and services "placed on the market in the Union" (lit. a) as well as to "offering such services to customers in the Union" the Data Act mirrors the well-known market principle. At first sight, the Data Act should be interpreted in line with existing data regulation – inter alia Art. 3(2)(a) and Rec. 23 GDPR as well as Art. 11(3) and Rec. 42 Data Governance Act (with its reference to "envisage offering services" (Rec. 23 GDPR)).[50]

Such a link to the EU internal market is also important for lit. b and d – as otherwise Art. 1(2) would lead to an "endless" territorial scope. Consequently, Art. 1(2)(d) should not be read in such a way that public sector bodies may request data from any data holder in the world.[51] At least, the wording of lit. b and d is insofar unclear as, in addition, Art. 2(6) does also not restrict the definition of data holders (at least for non-personal data) to a specific territory.

The Council Presidency adds an "irrespective of their place of establishment" to the definitions set out in Art. 1(2)(a), (b), (c), and (e) – underlining the extraterritorial approach of the Act.[52]

The Council Presidency also proposes to add a new Art. 1(2)(f) clarifying that "operators within data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of agreements to make data available" are within the personal scope of the Act.[53]

Conflicting Regulatory Instruments / Competences of the Member States / Sector-Specific Rules

---

[47] Cf. the (different) terminology and the concept sub Ch. 6 below.

[48] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[49] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[50] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[51] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[52] Council Presidency 2022/0047(COD) – 13342/22, p. 35.

[53] Council Presidency 2022/0047(COD) – 13342/22, p. 36.

Rec. 4 clearly tackles the inherent question of competence. The recitals states that Member States "should not adopt or maintain additional national requirements on those matters falling within the scope of this Regulation" in order to guarantee the "direct and uniform application" of the Act. Exceptions must be explicitly named within the Act. This is the case inter alia the case in Art. 18(2) pointing to sectoral legislation.

Only within the recitals (Rec. 24), it becomes apparent that the Act allows – in the context of the compulsory data licence agreement according to Art. 4(6) – for rather broad sector-specific deviations[54]:

> "This Regulation should also not prevent sector-specific regulatory requirements under Union law, or national law compatible with Union law, which would exclude or limit the use of certain such data by the data holder on well-defined public policy grounds."

Rec. 25 elaborates:

> "In sectors characterised by the concentration of a small number of manufacturers supplying end users, there are only limited options available to users with regard to sharing data with those manufacturers. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers, making it difficult for users to obtain value from the data generated by the equipment they purchase or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in Europe. This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives."

Art. 1(4) Sentence 3 adds that the Act does not affect Member States competences with regard to "activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law."[55]

The Council Presidency goes a step further and stipulates:

> "This Regulation does not apply to activities or data in areas that fall outsi[d]e the scope of Union law and in any event shall not affect the competences of the Member States regarding activities or data concerning public security, defence or national security, regardless of the type of entity carrying out the activities or processing the data, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order. This Regulation shall not affect the

[54] Cf. Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (955); Specht-Riemenschneider, L., *MMR* 2022, 809 (811). Demanding respective rules from an Economics perspective, Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 15; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 6. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 78.

[55] Cf. also Rec. 9 (identical Rec. 13).

> competences of the Member States regarding activities or data concerning customs and tax administration and the health and safety of citizens."[56]

The Council Presidency also proposes an addendum to Rec. 4 regarding trade agreements: "Moreover, action at Union level should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union."[57]

Additionally, the Council Presidency clarifies in a new Art. 1(4) Sentence 1 that "This Regulation does not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities."[58]

2. Interplay with Existing Rules (Art. 1 paras. 3 and 4, Art. 35)[59]

Manifold questions arise regarding the interplay of the Data Act with existing rules in other fields of laws.[60]

Intellectual Property Law[61]

Fundamentally, Art. 35 curbs protection granted to databases by way of a *sui generis* right within the ambit of the Proposal. Art. 7 of Directive 96/9/EC (Database Directive)[62] shall not apply to databases containing data obtained from or generated by the use of a product or a related service. Aim is to not to hinder the exercise of the access (and use) right of users according to Art. 4 and the right to share such data with third parties according to Art. 5.[63]

However, the scope of Art. 35 remains unclear.[64] Especially, as Rec. 84 underlines that the Data is seeking to "eliminate the risk that holders of data (…) claim" the *sui generis* right "where such databases do not qualify for the *sui generis* right, and in so doing hinder the effective exercise" of the user's rights – and, in addition, states that "this Regulation should clarify that the *sui generis* right does not apply to such databases as the requirements for protection would not be fulfilled".

The Council Presidency proposes "For the purposes of the exercise of the rights provided for in Art. 4 and 5 of this Regulation, the *sui generis* right provided for in Art. 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by a product or related

---

[56] Council Presidency 2022/0047(COD) – 15035/22, pp. 39 et seq.

[57] Council Presidency 2022/0047(COD) – 13342/22, p. 8.

[58] Council Presidency 2022/0047(COD) – 13342/22, p. 36.

[59] Questions of Trade Secrets Law are discussed below in the context of the relevant norms. Cf. in detail in this regard Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 100 n. 277 et seq. For question of Private International Law cf. ibid. pp. 120 et seq. n. 333 et seq.

[60] Cf. in detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 96 n. 267 et seq. See also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 73 et seq.

[61] Cf. in detail for intellectual property rights beyond Art. 35 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 96 n. 268 et seq. as well as Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 76.

[62] Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases.

[63] Cf. also Rec. 63.

[64] Cf. for a discussion in detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 90 n. 254 et seq.

service." Or "The *sui generis* right provided for in Art. 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by the use of a product or a related service."[65]

Data Protection Law[66]

The omnipresent question of the interplay between the Data Act – as applying to personal and non-personal data alike – and Data Protection Law sought to be answered by Art. 1(3). According to Art. 1(3) Sentence 2, the Data Act shall not affect the applicability of Union law on the protection of personal data, in particular the GDPR and Directive 2002/58/EC (ePrivacy Directive)[67] (including the powers and competences of supervisory authorities). Rec. 7 confirms that these acts (as well as the Regulation (EU) 2018/1725[68] mentioned here) "provide the basis for sustainable and responsible data processing, including where datasets include a mix of personal and non-personal data".

The Data Act obligations are – as far as the processing of personal data is concerned – added to the existing Data Protection Law duties of processors.[69] Rec. 7 explicitly underlines that "[n]o provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications."[70] Rec. 24 confirms additionally: "Insofar as personal data are processed, the data holder should be a controller under [the GDPR]." In many cases, it needs to be evaluated carefully whether and to what extent a joint controllership (Art. 26 GDPR) exists.[71]

Rec. 8 additionally highlights the Data Protection Law principles of data minimisation and data protection by design and by default as well as the technical and organisational measures going along with these principles (cf. inter alia Art. 24 and 32 GDPR). With respect to respective measures Rec. 8 insists that "[s]uch measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves."

Against this background, the Council Presidency, first, adds a reference to "national [data protection] law". Second, it is added:

> "This Regulation is without prejudice to, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities. Insofar as data subjects are concerned,

[65] Council Presidency 2022/0047(COD) – 13342/22, p. 68.

[66] Cf. for a discussion in detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 105 et seq. n. 291 et seq.

[67] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[68] Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

[69] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 91.

[70] But cf. Art. 18(5) and 21 (sub VII. 6. and 9.).

[71] Cf. in this regard Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 90 et seq., 99.

> the rights laid down in Chapter II of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679. And shall not adversely affect data protection rights of others. "[72]

JURI is proposed to clarify in Art. 1(3) that the priority of data protection law shall also apply "where datasets include a mix of personal and non personal data".[73]

In Particular: Legal Basis According to Art. 6(1)(c) and (3) GDPR

One of the main disputes around the Data Act is concerning whether and to what extent the Act obligations, especially to grant access, are to be read a constituting a legal obligation according to Art. 6(1)(c) (as well as Art. 6(1)(e) and (3)) GDPR – justifying the respective data processing (transfer to user and / or third party) that inevitable required for the fulfilment of the respective obligations.[74] It is obvious that route taken in this regard is fundamentally shaping the effectiveness of the Data Act.[75] At least, if one really is willing to boost data sharing and data use by the means – and safeguards! – proposed by the Act (especially by Art. 4 et seq. and Art. 14 et seq.), it is favourable to regard the Act's obligations as a respective legal basis according to Art. 6(1)(c) and (3).

If the obligations of the Act would not constitute a respective legal basis, data holders will in many cases not be able to establish a(nother) legal basis for the data processing – especially, if the user is not the data subject and /or if it cannot be excluded that personal data of other data subjects are at stake.[76] Only, in the rather simple case that the user = data subject is requesting the data and / or is requesting a transfer to a third party, this request will easily be framed as or connected with a consent of the respective data subject. Relying on a reference to Art. 6(1)(f) GDPR will in many cases not deliver the needed degree of legal certainty.[77]

The Council Presidency has made several proposals – still highly debated[78] – to clarify this question. It is fair to say that at this moment in time many uncertainties remain and the final version is yet to be drafted. In its compromise text, the Council Presidency added different aspect in Rec. 5, 24, 61, and 64 as well as in Art. 17(1)(d).[79]

With regard to the access regime in Art. 4 et seq.:

> "This Regulation should not be interpreted as recognising or creating any legal basis in accordance with Article 6(1)(c) and 6(3) of Regulation (EU) 2016/679 for the purpose of allowing the data holder to hold, have access to or process data, or as conferring any

---

[72] Council Presidency 2022/0047(COD) – 15035/22, p. 39.

[73] JURI PE736.696, p. 26.

[74] Strongly in favour Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 90 et seq.; Specht-Riemenschneider, L., *MMR* 2022, 809 (810 et seq.).

[75] Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 75.

[76] Cf. Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 76, 91.

[77] Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 90; Specht-Riemenschneider, L., *MMR* 2022, 809 (811).

[78] Cf. also the proposal by LIBE, PE737.389, pp. 23 et seq.

[79] Council Presidency 2022/0047(COD) – 15035/22, p. 2.

> new right on the data holder to use data generated by the use of a product or related service." (Rec. 5)[80]
>
> "This Regulation imposes the obligation on data holders to make data available in certain circumstances, in accordance with Article 6(1)(c) and 6(3) of Regulation (EU) 2016/679. (…) Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation. However, this Regulation does not create a legal basis in accordance with Article 6(1)(c) and 6(3) of the under Regulation (EU) 2016/679 that imposes on the data holder an obligation to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder." (Rec. 24)[81]

With regard to the access regime in Art. 14 et seq.:

> "In accordance with Article 6(1) and 6(3) of Regulation (EU) 2016/679, a proportionate, limited and predictable framework at Union level is necessary when providing for the legal basis for the making available of data by data holders, in cases of exceptional needs, to public sector bodies and to Union institution, agencies or bodies." (Rec. 61)[82]

In Particular: Art. 20 GDPR

Art. 1(3) Sentence 3 confirms that in particular the right to data portability remains untouched ("complements") by what is prescribed in Chapter II of the Act – despite the similar nature of the right to access according to Art. 4(1) and 5(1). Interestingly, no such complementary relationship with Art. 20 GDPR is stated for the rights in relation to switching between data processing services under Chapter VI of the Act.[83]

Data Governance Act

Whilst the Commission proposal was rather silent on the interplay with the DGA (cf. only Rec. 35), the Council Presidency now rightly points to the fact that:

> "Data intermediation services [as regulated by Regulation (EU) 2022/868] may support users or third parties in establishing a commercial relation for any lawful purpose on the basis of data of products in scope of this Regulation e.g. by acting on behalf of a user. They could play an instrumental role in aggregating access to data from a large number of individual users so that big data analyses or machine learning can be facilitated, as

[80] Council Presidency 2022/0047(COD) – 15035/22, pp. 8 et seq.

[81] Council Presidency 2022/0047(COD) – 15035/22, pp. 14 et seq.

[82] Council Presidency 2022/0047(COD) – 15035/22, p. 25.

[83] Cf. Lienemann, G. / Wienroeder, M., Part III (Art. 23-34, 36-42), in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (Eds.). The Data Act Proposal – Literature Review and Critical Analysis (University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-03), 2023, p. 9 et seq.

> long as such users remain in full control on whether to contribute their data to such aggregation and the commercial terms under which their data will be used."[84]

This is not to say that this recital is sufficient. The Data Act does not substantially tackle the relationship to and its interplay with the Data Governance Act (DGA).[85] Specific rules are missing and no incentives are set (for example to the benefit data intermediaries). As data intermediaries do fulfil a central function in order to enable data exchanges / data contracts, this gap fundamentally opposes the general aim of the Data Act to enhance and foster data sharing and data use.

Only minor aspects with regard to public sector information and with regard to the European Data Innovation Board are now proposed by the Council Presidency (Art. 17(3), 27(3), 34a).[86]

Free Flow of Data-Regulation

The Council Presidency points to in a new Art. 1(4a):

> "This Regulation adds generally applicable obligations on cloud switching going beyond the self-regulatory approach of Regulation (EU) 2018/1807 on the free flow of non-personal data in the European Union."[87]

Competition Law

According to Rec. 88, the Data Act does not touch Competition Law (Art. 101 et seq. TFEU).[88] The instruments spelled out in the Act shall not be used in way that does not comply with Art. 101 et seq. TFEU.[89]

Criminal Law / Criminal Procedural Law / Digital Services Act

Art. 1(4) Sentence 1 states in addition that the Act shall not affect "Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties". This shall include Regulation (EU) 2021/784[90], the e-evidence proposals[91] (once adopted), and international cooperation in this regard (Rec. 10 refers to the Budapest

---

[84] Council Presidency 2022/0047(COD) – 15035/22, p. 16.

[85] Cf e.g., Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 236.

[86] Council Presidency 2022/0047(COD) – 15035/22, pp. 16, 56, 64, 71 et seq.

[87] Council Presidency 2022/0047(COD) – 13342/22, p. 36.

[88] Cf. also on the question whether Competition Law instruments are granting adequate solutions for the situations tackled by the Data Act Proposal Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 17 et seq. n. 36 et seq.

[89] Cf. also Bomhard, D. / Merkle, M., *RDi* 2022, 168 (172).

[90] Regulation (EU) 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online.

[91] COM(2018) 225 final and COM(2022) 226 final.

Convention[92] in particular). Art. 1(4) Sentence 2 similarly carves out the Directive (EU) 2015/849[93] and Regulation (EU) 2015/847[94].

(Only) Rec. 10 adds Regulation (EU) 2022/2065 (Digital Services Act)[95] in this respect.

Rather broadly, the Council Presidency proposes an addendum to the carve-outs by Art. 1(4) by suggesting to not affect competences "to safeguard (…) essential State functions, including ensuring the territorial integrity of the State and maintaining law and order".[96]

Contract Law

The Council Presidency proposes to clarify in Rec. 9 that the Data act "should not affect national general contract laws such as rules on formation, the validity or effects of contracts, including the consequences of the termination of a contract."[97]

Unfair Terms

The question whether and to what extend the Data Act should include rules on unfair terms also in b2-c-constelltions is highly disputed. The Council Presidency – in line with the Proposal – takes a negative stand – expressly stating in a new Art. 1(4b): "This Regulation does not affect Directive 93/13/EEC on Unfair Terms in Consumer Contracts."[98]

Consumer Law

Rec. 9 confirms that the Act "complements and is without prejudice to Union law aiming to promote the interests of consumers and to ensure a high level of consumer protection, to protect their health, safety and economic interests". In detail, the Directive 2005/29/EC (Unfair Commercial Practices Directive)[99], the Directive 2011/83/EU[100], and the Directive 93/13/EEC[101] are mentioned.

---

[92] Council of Europe 2001 Convention on Cybercrime.

[93] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

[94] Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying the transfer of funds.

[95] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services.

[96] Council Presidency 2022/0047(COD) – 13342/22, p. 36.

[97] Council Presidency 2022/0047(COD) – 15035/22, p. 9.

[98] Council Presidency 2022/0047(COD) – 13342/22, p. 37.

[99] Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market.

[100] Directive 2011/83/EU of the European Parliament and of the Council on consumer rights.

[101] Directive 93/13/EEC on unfair terms in consumer contracts. Directive (EU) 2019/2161 of the European Parliament and of the Council amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/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.

It is further proposed to include explicitly the Directive (EU) 2019/771[102].[103]

Product Safety / Accessibility Requirements for Products and Services

Rec. 11 and 12 confirms respectively that product-specific regulations regarding physical design and data requirements as well as accessibility requirements on certain products and services (in particular Directive 2019/882[104]) shall remain unaffected.

3. Definitions (Art. 2)

Art. 2 defines the Act's central terms. Within the legislative process, various further definitions have been proposed, e. g. for personal data, non-personal data, consent, data subject, customer etc.[105]

Data

According to Art. 2(1) data means any digital representation of acts, facts or information and any compilation[106] of such acts, facts or information, including in the form of sound, visual or audio-visual recording.[107] Data therefore encompasses personal as well non-personal data. This definition is a sensible one – as it does not just equal data to information (as Art. 4(1) GDPR) does.[108] It is underlined that data are "transporters" of information.[109]

Rec. 14 adds that the scope of the Act is focused on "data [that] represent the digitalisation of user actions and events (…), while information derived or inferred from this data, where lawfully held, should not be considered within scope".

It is especially notable that the Council Presidency has proposed a definition for "data generated the use"[110] (a notion discussed in detail below[111]) – being the key factor for the data access regime according Art. 4 et seq. Art. 2(1af) shall read

> "'data generated by the use of a product or a related service' means data recorded intentionally by the user or as a by-product of the user's action, as well as data generated or recorded during the period of lawful use among others in standby mode or while the

[102] 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.

[103] Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 30 et seq. n. 74.

[104] Directive (EU) 2019/882 of the European Parliament and of the Council on the accessibility requirements for products and services.

[105] Council Presidency 2022/0047(COD) – 13342/22, p. 37; Council Presidency 2022/0047(COD) – 15035/22, pp. 40 et seq.; JURI PE736.696, pp. 27 et seq.; LIBE, PE737.389, pp. 25 et seq.

[106] Cf. regard this rather vague term Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 23 n. 57.

[107] Similar to ISO-Norm ISO/IEC 2382:2015, IT Vocabulary, 2121272. Cf. also in general Zech, H. Information als Schutzgegenstand, 2012, p. 32 et seq.; Zech, H., Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", *CR* 2015, 137 (138 et seq.).

[108] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[109] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[110] Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 14 et seq. n. 30.

[111] See IV. 1.

> product is switched off. This does not include the results of processing that substantially modifies the data;"[112]

Product

According to Art. 2(2) product means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available[113] electronic communications service[114] and whose primary function is not the storing and processing of data. This definition mainly refers to Internet of Things-products.[115] Rec. 14 confirms and clarifies in this regard:

> "Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. (…) Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery."

Rec. 15 stipulates examples / categories of products that are not covered:

> "In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps."

The term "product" is primarily used in the context of the data sharing regime under Chapter II (Art. 3 through 7) but also appears in passing within the exclusion of applicability regarding Directive 1996/9/ EC under Art. 35.

As the borderline drawn by the Commission proposal is not entirely clear[116], the Council Proposal has proposed several clarifying amendments to the aforementioned parts of the Act.[117] A product is additionally defined as being "able to communicate data directly or indirectly" and as not being "primarily designed to display or play content, or to record and transmit

---

[112] Council Presidency 2022/0047(COD) – 15035/22, p. 40.

[113] Cf. in this regard Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 82.

[114] Rec. 14 explains that „[e]lectronic communications services include land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks."

[115] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[116] Cf. Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170); Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 25; Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 82 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 23 et seq. n. 58.

[117] Council Presidency 2022/0047(COD) – 15035/22, pp. 10 et seq. and 40 et seq.

content".[118] According to the Council Presidency's proposal for Rec. 15 products shall therefore not include:

> "smart televisions and speakers, cameras, webcams, sound recording systems and text scanners. Additionally, products primarily designed to process and store data, such as personal computers, servers, tablets and smart phones, should not fall in scope of this Regulation."[119]

According to the Council Presidency's proposal for Rec. 15 covered are "[o]n the other hand, smart watches have a strong element of collection of data on human body indicators or movements".[120]

Related Service

According to Art. 2(3) related service means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from per-forming one of its functions.[121]

The term "related service" is primarily used in the context of the data sharing regime under Chapter II (Art. 3-7) but also appears in passing within the exclusion of applicability regarding Directive 1996/9/EC under Art. 35.

Virtual Assistants

According to Art. 2(4) virtual assistants means software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices.[122]

User

According to Art. 2(5) user means a natural or legal person that owns, rents or leases a product or receives a service. The Council Presidency clarifies that a user includes a data subject.[123]

This definition is rather obscure.[124] It is unclear whether the user is defined by the contractual relationship (lease, rent) or by an actual legal position (ownership). It is therefore debated whether and to what extent the user position rests on a factual situation (e. g., possession), a qualified factual situation (e. g., possession with a respective title), or on a contractual basis only.[125]

---

[118] Council Presidency 2022/0047(COD) – 15035/22, pp. 40 et seq.

[119] Council Presidency 2022/0047(COD) – 15035/22, p. 11.

[120] Council Presidency 2022/0047(COD) – 15035/22, pp. 11 et seq.

[121] Cf. for proposals to amend Council Presidency 2022/0047(COD) – 15035/22, p. 41.

[122] Cf. for proposals to amend Council Presidency 2022/0047(COD) – 15035/22, p. 41. Cf. also the proposed Art. 1(2a) at Council Presidency 2022/0047(COD) – 15035/22, p. 39 (deleting Art. 7(2) at the same time).

[123] Council Presidency 2022/0047(COD) – 15035/22, p. 41.

[124] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 24 n. 59 et seq.

[125] Cf. for a detailed discussion Specht-Riemenschneider, L., *MMR* 2022, 809 (813 et seq.).

Rec. 18 of the Council Presidency proposal therefore reads:

> „The user of a product should be understood as the legal or natural person, such as a business or consumer, but also a public sector body, that owns, rents or leases the product on other than short-term basis. Depending on the legal title under which he uses it, such a user bears the risks and enjoys the benefits of using the connected product and should enjoy also the access to the data it generates. The user should therefore be entitled to derive benefit from data generated by that product and any related service. An owner, renter or lessee should equally be considered as user, including when several entities can be considered as users. In the context of multiple users, each user may contribute in a different manner to the data generation and can have an interest in several forms of use, e.g. fleet management for a leasing company, or mobility solutions for individuals using a car sharing service."[126]

Furthermore, it remains unclear how to deal with scenarios where different person must be considered as user (e. g. owner, lessor, driver, regular driver etc. for a smart car).[127]

While the definition for "user" is relied upon at various points throughout the Proposal (namely in Art. 3-6, Art. 8, Art. 11, Art. 31, Art. 35, and Art. 40), it is used particularly often in the context of user-held access and sharing rights under Chapter II.

Data Holder

According to Art. 2(6) data holder means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data. This definition is rather unclear, at least extremely wide as it only relies on the ability to make data available.[128] Furthermore, it becomes apparent that the data holder might evade access obligations by deleting the data in question.[129] Consequently, it is partly argued that the user shall be notified before deletion and granted a possibility to access the data.[130]

The Council Presidency proposes instead:

> "'data holder' means a legal or natural person who
>
> - has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, to make available certain data or
>
> - can enable access to the data through control of the technical design or means of access, in the case of non-personal data;"[131]

---

[126] Council Presidency 2022/0047(COD) – 15035/22, p. 12.

[127] Cf. in this regard below sub IV. 1. and Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170).

[128] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (169). In contrary to Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 25 n. 62.

[129] Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

[130] See Specht-Riemenschneider, L., *MMR* 2022, 809 (815). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 25 n. 62.

[131] Council Presidency 2022/0047(COD) – 15035/22, p. 41.

Rec. 30 additionally points to the fact that the user after having exercised its right to access might become a data holder[132]:

> "It should be understood that such a user, once data has been made available, may in turn become a data holder, if they meet the criteria under this Regulation and thus become subject to the obligations to make data available under this Regulation."

Like with "data user", the term "data holder" is a constant presence throughout vast parts of the Proposals, appearing in Art. 3-5, Art. 8-9, Art. 11-12, Art. 14, Art, 17-22, and in Art. 27.

Data Recipient

According to Art. 2(7) data recipient means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law.

The term "data recipient" is exclusive to the obligations placed on data holders under Chapter III (Art. 8-12) of the Proposal.

Enterprise

According to Art. 2(8) enterprise means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession.

The definition for "enterprise" is both relevant in the context of privileges and exemptions afforded to micro, small, or medium-sized enterprises (Art. 7-9, Art. 13-14; cf. the dedicated definition under Art. 2 of the Annex to Recommendation 2003/361/EC) as well as in other respects: Art. 8(3) mentions enterprises as a category of data recipients, Art. 13 as the contractual counterpart, and Art. 41 as excluded beneficiaries of the right to share data under Art. 5 (likely beyond gatekeepers within the meaning of the DMA, which are already barred from receiving data pursuant to Art. 5(2)(c)).

Public Sector Body

According to Art. 2(9) public sector body means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies.

The term "public sector body" is exclusive to Chapter V (Art. 14-22).

Public Emergency

According to Art. 2(10) public emergency means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s).[133]

---

[132] In addition, data holder and user might be joint controllers according to Art. 26 GDPR, cf. Rec 30.

[133] Cf. for proposed amendments Council Presidency 2022/0047(COD) – 15035/22, p. 41.

Likewise, the term "public emergency" is exclusive to Chapter V and is only used in Art. 15, Art. 18, and Art. 20.

Processing

According to Art. 2(11) processing means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Given its foundational meaning within the jargon of data (protection) law (cf., most notably, Art. 4(2) GDPR), it comes as a surprise that the Proposal only draws on the definition for "processing" on two occasions, namely in the context of purpose-specificity (Art. 6(1)) and of necessity (Art. 19(1)(b)).

Data Processing Service

According to Art. 2(12) data processing service means a digital service other than an online content service as defined in Art. 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature. On the one hand, the exclusion of online content services as per Art. 2(5) of the Portability Regulation (EU) 2017/1128 means that a sizeable number of online platforms, namely those providing linear (i.e. scheduled) broadcasting or non-linear (i.e. on-demand) music and video streaming services[134] will not be considered data processing services. On the other hand, because outwards scalability and elasticity of computing resources according to fluctuating demand are an essential property of cloud computing in general[135], a plethora of service models will fall firmly within the definition under Art. 2(12). Rec. 71 and 72 corroborate this rather wide-ranging impetus by recognising virtual IT infrastructure, most notably virtual machines, as a relevant type of computing resource.

The use of the term "data processing service" extends beyond the switching requirements of Chapter VI (Art. 23-26) to the associated interoperability standards under Art. 29 (see also Art. 41) and to the restrictions on transfers of non-personal data under Art. 27.

Service Type

According to Art. 2(13) service type means a set of data processing services that share the same primary objective and basic data processing service model.

The term "service type" appears in Art. 23, Art. 26, and in Art. 29.

Functional Equivalence

According to Art. 2(14) functional equivalence means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process,

---

[134] Engels, S. / Nordemann, J.B., The Portability Regulation (Regulation (EU) 2017/1128) – A Commentary on the Scope and Application. 9 (2018) *JIPITEC* 179 para 22.

[135] Cf. the conceptualisation, by now classical, put forth by Mell, P. / Grance, T., The NIST Definition of Cloud Computing (*NIST Special Publication* 800-145, 2011), p. 2.

to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract. The Proposal remains silent on the question which specific components of a given service constitute its core elements and, conversely, which elements are of ancillary or secondary importance to overall functionality. Whilst attempts to pinpoint the core elements of multi-purpose business cloud platforms (e.g., AWS, Microsoft Azure, or Salesforce) would have been largely futile, examples based on less complex service types such as cloud storage could have shed some light on what functional equivalence actually entails.

The term "functional equivalence" appears in Art. 23, Art. 26, and Art. 29.

Open Interoperability Specifications

According to Art. 2(15) open interoperability specifications mean ICT technical specifications (i.e. those in the field of information and communication technologies), as defined in Regulation (EU) No 1025/2012, which are performance oriented towards achieving interoperability between data processing services.

The term "open interoperability specifications" appears in Art. 26 and Art. 29.

Smart Contract

According to Art. 2(16) smart contract means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger.

The definition for "smart contracts" is chiefly relied upon (and put into concrete terms) in Art. 30, the requirements of which are incorporated into Art. 28(1)(d). Moreover, smart contracts are suggested as a protective measure against unauthorised disclosure of data pursuant to Art. 11(1).

Electronic Ledger

According to Art. 2(17) electronic ledger means an electronic ledger within the meaning of Art. 3, point (53), of Regulation (EU) No 910/2014. The definition erroneously refers to the wording incorporated into Regulation (EU) 910/2014 by a June 2021 amending proposal[136] as current law – which is not yet the case as of November 2022.

Curiously, this definition is merely of auxiliary importance, i.e. to define a term within the overarching definition for "smart contracts", and is not used anywhere else in the Proposal.

Common Specifications

According to Art. 2(18) common specifications means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation.

The term "common specifications" is employed in the context of standard-setting towards interoperability between data spaces (Art. 28(5)) and for smart contracts (Art. 30(6)). On both

[136] Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity' COM(2021) 281 final.

points, the Commission may adopt delegated legislation in accordance with Art. 38 or Art. 39, respectively.

Interoperability

According to Art. 2(19) interoperability means the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions. This definition, which borrows from long-standing jargon in computing science[137], is construed for broader purposes than the one given in Art. 2(12) of Directive (EU) 2019/770 (Digital Content Directive)[138] and essentially applies to digital IT infrastructure *in toto*, addressing their ability to exchange data on multiple levels of abstraction (→ Art. 29(2)(a)).

The term "interoperability" is mainly used in Art. 28 and Art. 29, but mention of the concept is also made in Art. 26(3) by way of reference to European standards for interoperability under Art. 29(5).

Harmonised Standard

According to Art. 2(20) harmonised standard means harmonised standard as defined in Art. 2, point (1)(c), of Regulation (EU) No 1025/2012.

The definition for "harmonised standard" is drawn on in Art. 28 and Art. 30.

[137] Cf., e.g., ISO-Norm ISO/IEC 19941:2017, Information technology — Cloud computing — Interoperability and portability (quoted directly in Recital 76); IEEE Standard Glossary of Software Engineering Terminology (1990), p. 42.

[138] Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services.

IV. Access to and Sharing of Data Generated by the Use of Products and Related Services (Art. 3-7)

Chapter II ('Business to Consumer and Business to Business Data Sharing', Art. 3-7)[139] is intended to increase legal certainty for consumers and businesses to access data generated by the products or related services they own, rent or lease.[140]

Users are afforded rights to access said data and request sharing to third parties and are hence attributed with *de facto*-entitlements over the data at hand.[141] Conversely, limitations are placed on data holders and data recipients when it comes to (secondary) use of the data.

1. Product and Service Design (Art. 3(1)), Data Generated by the Use

According to Art. 3(1) products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user. Art. 7(2) highlights that respective products and services might also encompass virtual assistants "insofar as they are used to access or control a product or related service".[142]

Generated By Its Use

Of central importance is the notion of *data generated by their (its) use* (cf. also Art. 4(1)).[143] Rec. 17 is of assistance to determine the rather opaque notion[144] of 'generated by'. Rec. 17 refers to different scenarios all of which are covered:

> (1) "data recorded intentionally by the user";
>
> (2) "data generated as a by-product of the user's action, such as diagnostics data,
>
> (3) "[data generated] without any action by the user, such as when the product is in 'standby mode';
>
> (4) "data recorded during periods when the product is switched off".

Rec. 17 further clarifies that "[s]uch data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights."[145] It has been noted that the different scenarios set out in Rec. 17

[139] The Council Presidency proposes "Right of Users To Use Data of Connected Products and Related Services" as title of the Chapter, cf. Council Presidency 2022/0047(COD) – 15035/22, p. 43.

[140] Commission, COM(2022) 68 final Explanatory Memorandum, p. 14.

[141] For further details cf. Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[142] Cf. also the proposed Art. 1(2a), Council Presidency 2022/0047(COD) – 15035/22, p. 39 (deleting Art. 7(2) at the same time).

[143] Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 84.

[144] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170).

[145] Cf. also Rec. 14 and above on the definition of data (sub III. 3. Data).

do not exactly match the statements on products covered and not-covered in Rec. 14.[146] Furthermore, it is argued that the reference to the software process and potentially infringed intellectual property rights is rather unsound in most cases.[147]

The proposal by the Council Presidency – deleting Rec. 17 and inserting it with the same wording as a "new" recital 14a[148] – does not fully solve this problem, but make a step into the right direction.

The Council Presidency has proposed a definition for "data generated the use" in Art. 2(1af):

> "'data generated by the use of a product or a related service' means data recorded intentionally by the user or as a by-product of the user's action, as well as data generated or recorded during the period of lawful use among others in standby mode or while the product is switched off. This does not include the results of processing that substantially modifies the data;"[149]

The Council Presidency adds in a proposed (and revised in parts) Rec. 14a:

> "In scope are data which are not substantially modified, meaning data in raw form (also known as source or primary data, which refers to data points that are automatically generated without any form of processing) as well as prepared data (data cleaned and transformed for the purpose of making it useable prior to further processing and analysis). The term 'prepared data' should be interpreted broadly, without however reaching the stage of deriving or inferring insights. Prepared data may include data enriched with metadata, including basic context and timestamp to make the data usable, combined with other data (e.g. sorted and classified with other data points relating to it) or re-formatted into a commonly-used format."[150]

However, the Council Presidency wants to limit the scope of Art. 3(1) to the extent that it only applies to data that is "readily available" to the data holder.[151] According to the proposed Art. 2(1ae), "readily available" shall mean

> "data generated by the use of a product that the data holder obtains or can obtain without disproportionate effort, going beyond a simple operation;"[152]

This limitation seems to be too vague and opens up potential for abuse.

Derived and Inferred Data

---

[146] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (169 et seq.). Cf. also Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 11 et seq.

[147] Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 13 et seq. n. 29.

[148] Council Presidency 2022/0047(COD) – 13342/22, pp. 10 et seq. as well as Council Presidency 2022/0047(COD) – 15035/22, p. 11.

[149] Council Presidency 2022/0047(COD) – 15035/22, p. 40.

[150] Council Presidency 2022/0047(COD) – 15035/22, p. 11.

[151] Council Presidency 2022/0047(COD) – 13342/22, p. 39.

[152] Council Presidency 2022/0047(COD) – 15035/22, p. 40.

It is furthermore highly disputed whether and to what extent "derived and inferred data" may be made accessible.[153] This is advocated for in the Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs (LIBE).[154]

The Council Presidency explicitly denies such a broad access in a proposed (and revised in parts) Rec. 14a:

> "(…) the results of processing that substantially modifies the data, i.e. information derived from this data, or information inferred from the original data, should not be considered within scope of this Regulation. Such data is not generated by the use of the product, but is the outcome of additional investments into taking insights from the data in terms of characterisation, assessment, recommendation, categorisation or similar systematic processes that assign values or insights and may be subject to intellectual property rights."[155]

Rec. 19 states correctly that "not all data generated by products or related services are easily accessible to their users" and that "there are often limited possibilities for the portability of data generated by products connected to the Internet of Things".[156] Due to that fact Art. 3(1) ensures in technical terms "that users of a product or related service in the Union can access, in a timely manner, the data generated by the use of that product or related service and that those users can use the data, including by sharing them with third parties of their choice".[157] By enabling "data access by default", Art. 3(1) creates the technical basis for an effective exercise of the rights under Art. 4 et seq.[158]

This shall simplify, for example, "switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union".[159] To allow developers to respond to the "far-reaching"[160] requirements of Art. 3(1), one might consider that the Act shall only apply to newly introduced products.[161]

Mechanisms of Access

In line with these goals, products "shall" be manufactured and services must be provided in such a way that the user-generated data can be accessed easily, securely and, if necessary,

---

[153] Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 23: Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 10 et seq. n. 20 et seq.

[154] LIBE PE737.389, p. 31.Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 11 n. 25.

[155] Council Presidency 2022/0047(COD) – 15035/22, p. 11.

[156] Rec. 19.

[157] Rec. 5.

[158] Cf. Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[159] Rec. 5.

[160] Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 5.

[161] Cf. BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 12.

directly.[162] These requirements are rather vague.[163] It has been partly argued that Art. 3(1) is to be understood more as a general principle and less as an enforceable claim.[164]

First and foremost, it is discussed whether and to what extent the Data Act allows a mere *in-situ* access of the user.[165] Partly, it is strongly argued with reference to Rec. 21 that the Act does not oblige the data holder to actually transmit the data in question, but under all circumstances may restrict its obligation to offering practically an interface only.[166] Others point to the difference between the *access by design*-obligation Art. 3 and the access right of Art. 4(1). Whilst Art. 3(1) shall be regarded as the general rule, Art. 4(1) – a rule that would otherwise not be necessary – shall offer a right to access that goes beyond *in-situ*.[167]

Rec. 20 states that when designing a product or connected service, it is important to ensure that, in the case of multiple contracting parties on the user side, each user[168] benefit equally from the measures of facilitated data access.[169] Regarding a product that is typically used by several persons, this includes, for example, the possibility of creating separate user accounts for individual users (which can be used by all users, if necessary)[170], thereby ensuring individual data management. Thereby, Art. 3(1) seeks to lay foundation for Art. 4(1) and (2) Sentence 2.

Rec. 20 refers to the fact that data shall be "granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder".[171]

The Council Presidency meaningfully suggests that the wording should be supplemented by an obligation to make the data available "free of charge".[172]

The restriction of the wording to allow data access only for cases where it is "relevant and appropriate" is irritating.[173] Rec. 21 only mentions therefore that "direct" availability refers to availability from an on-device data storage as well as from a remote server.[174] In line with the MPIIC, it is not clear why the reservation ("where relevant and appropriate") refers only to

---

[162] Cf. Rec. 19; Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[163] Gerpott, T., *CR* 2022, 271 (275).

[164] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 85.

[165] Cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 26 et seq. n. 65 et seq.

[166] See especially Specht-Riemenschneider, L., *MMR* 2022, 809 (815 et seq.).

[167] Pointing to the open formulation of Art. 4(1) Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (957). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 26 et seq. n. 66 and p. 32 n. 79. See – in contrary – Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

[168] Council Presidency 2022/0047(COD) – 15035/22, p. 13.

[169] Cf. Rec. 20.

[170] Rec. 20; this is also the direction of the proposal by Specht-Riemenschneider, L., *MMR* 2022, 809 (815).

[171] Rec. 20.

[172] Council Presidency 2022/0047(COD) – 13342/22, p. 40; concurringly ITRE PE732.704, p. 33.

[173] See also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 73.

[174] Rec. 21.

"direct" accessibility and not to easy and safe accessibility.[175] To avoid confusion, the phrase "where relevant and appropriate" should be deleted.[176]

It was suggested that the data should also be made available in a "in a structured, commonly used and machine-readable format".[177] The proposal is to be explicitly welcomed as it ensures that users can make use of the information provided. The LIBE Draft Opinion proposes to design products in such a way that data subjects can directly exercise their rights under Art. 15 et seq. GDPR[178] is also to be supported.

Personal Scope

Finally, the wording of Art. 3(1) does not make entirely clear what the relationship between Art. 3(1) and the underlying contract is as well as who is to be obliged by the provision.[179] Ultimately, this obligation can only affect the manufacturer.[180] All in all, the meaning of Art. 3(1) should be defined even more precisely in the recitals and in general.[181]

2. Information Duties (Art. 3(2))

According to Art. 3(2), the user shall be provided with at least the following information in a clear and comprehensible format before concluding a contract for the purchase, rent or lease of a product or a related service: the nature and volume of the data likely to be generated by the use of the product or related service (lit. a); whether the data is likely to be generated continuously and in real-time (lit. b); how the user may access those data (lit. c); whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used (lit. d); whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established (lit. e); the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently (lit. f); how the user may request that the data are shared with a third-party (lit. g); the user's right to lodge a complaint alleging a violation of the provisions of this chapter with the competent authority referred to in Art. 31(lit. h).

Personal Scope

Art. 3(2) does not specify who exactly is obliged to provide the information.[182] As the information duty must (only) be fulfilled vis-à-vis the user before concluding a contract, only the user's contractual partner can be obliged to provide information.[183] Nevertheless, the

[175] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 73.

[176] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 73.

[177] Council Presidency 2022/0047(COD) – 13342/22, p. 40; LIBE PE737.389, p. 31; ITRE PE732.704, p. 33.

[178] LIBE PE737.389, p. 31.

[179] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 74.

[180] In detail, Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 74.

[181] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 85.

[182] Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 31 n. 77.

[183] Cf. also Specht-Riemenschneider, L., *MMR* 2022, 809 (817).

Council Presidency regards the data holder as being obliged by the information duty and proposes an amendment to the wording to this effect.[184] This amendment is suboptimal, as the data holder will not always be identical to that of the contractual partner. In these cases, this would soften the obligation to provide the information to the disadvantage of the user. For reasons of practicability, only the seller, rentor or lessor should be obliged to provide the information.

However, the contractual partner is only responsible for the actual provision, but not for the content of the policy. Of course, the manufacturer must make the information available to the user's contractual partner and thus in the end also to all intermediate instances.[185] According to the wording, the information duties also apply in c2c-relationships[186], for example in a non-commercial resale of a smart product. Whether this was the Commission's intention is highly questionable. An exception for c2c-relationships should therefore be considered. Of course, in such situations, neither the data holder nor the primary contractual partner of the non-commercial re-seller can be held liable for the provision of the information.[187]

According to Art. 7(1), the information duties do not apply for data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Art. 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Art. 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise.

This exception is particularly useful for small(er) companies.[188] To ensure fair access to and use of data for such companies as well, they should not be unduly burdened by compliance with information duties.[189]

General Requirements for Providing Information

Art. 3(2) is only referring to a *provision* of information. The contractual partner of the user is not obliged to ensure that the information is actually acknowledged or understood by the user.

Rec. 23 sheds light on the purpose by stating that Art. 3(2) is intended to "provide transparency over the data generated and to enhance the easy access for the user". In this respect, Art. 3(2) deals on the one hand with the fear of losing (more and more) control over the use of one's "own" data[190].[191] At the same time, the user should be given the opportunity to reconsider the conclusion of the contract from a data-economic perspective on the basis of the information provided.[192] If the user comes to the result that the intended use is not compatible with his or

[184] Council Presidency 2022/0047(COD) – 13342/22, p. 40; according to the amended Rec. 23, the seller, rentor or lessor "acts as a messenger", Council Presidency 2022/0047(COD) – 15035/22, p. 14.

[185] Cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 31 n. 77.

[186] Seen differently by Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 31 n. 77.

[187] Cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 31 et seq. n. 77.

[188] Ebner, G., *ZD* 2022, 364 (367).

[189] Cf. Rec. 5.

[190] Commission, Special Eurobarometer 487a "The General Data Protection Regulation", 2019 (39).

[191] Ebner, G., *ZD* 2022, 364 (367).

[192] Cf. Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

her valuation of the contractual bargain, the conclusion of the contract can still be prevented in time.[193]

Art. 3(2) merely states that the information must be provided before the contract is concluded. Neither in Art. 3(2) nor in the recitals[194] are any further references given to a specific time of information. In any case, it would at least be useful to provide the information not just before the conclusion of the contract, but at a sufficient time before the contract is finalised[195] in order to be able to reflect the conclusion of the contract sufficiently. At the same time, due to the different application situations, it is also not possible to specify general time periods for the fulfilment of the information duty.

In its proposed amendment to Rec. 23, the Council Presidency suggests that users should be informed of changes in any information during "the lifetime of a product".[196] The amendment is positive from a user's perspective. However, it is questionable how the average lifetime of certain products is to be determined. In this respect, the determination of a general period of approximately five years could be appropriate. Also, a corresponding provision should be included in Art. 3(2).

According to the wording of Art. 3(2) ("purchase, rent or lease"), one might argue that the information duty only applies before concluding contracts with a *monetary consideration*.[197] Cases in which products are handed over entirely without monetary consideration should be rare, but nevertheless cannot be excluded. It was therefore already rightly mentioned that this wording of Art. 3(2) leaves room for avoiding the information duty when products are provided at no cost[198], for example in the case of a free trial use of a product. Needless to say, that the information in Art. 3(2) is, however, relevant, after all, when using the product, regardless of whether a contract with a monetary consideration has been concluded. At least, if instead of a monetary payment the generated data is actually constituting the counter-performance (according to the prevailing understanding[199] data can constitute consideration[200]), the threshold "purchase, rent or lease" is met – and Art. 3(2) applies.

The Council Presidency proposes for Rec. 23 that "it is in any case necessary that the user is enabled to store the information in a way that is accessible for future reference and that allows the unchanged reproduction of the information stored".[201]

According to Art. 3(2) the information must be provided in a clear and comprehensible format. Rec. 23 adds to these requirements that sufficient information is also provided on how the data generated may be accessed. Even if this criterion seems to extend only to the information on

---

[193] Ebner, G., *ZD* 2022, 364 (367).

[194] The latest amendment of the Council Presidency also refers to the time before concluding a contract in Rec. 23, see Council Presidency 2022/0047(COD) – 15035/22, p. 14.

[195] Ebner, G., *ZD* 2022, 364 (367).

[196] Council Presidency 2022/0047(COD) – 15035/22, p. 14.

[197] Cf. Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173).

[198] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173).

[199] Cf. Art. 3(2) Digital Content Directive and § 327 BGB.

[200] Alternatively, the conclusion of the data licence agreement according to Art. 4(6) Sentence 1.

[201] Council Presidency 2022/0047(COD) – 15035/22, p. 14.

the existence of the right of access to data, it must be assumed that all information under Art. 3(2) must be provided to a sufficient extent.

Nevertheless, it becomes quickly apparent that the requirements of these formal requirements lag far behind what is required by Art. 12(1) and (7) GDPR.[202] This is generally unfortunate. Insights from a behavioural economic analysis of Art.12-14 GDPR and privacy notices based thereon in particular point to the fact that relevant information must be communicated in a short and concise manner and in a way that is easy to comprehend.[203] Otherwise, there is a high probability that the information will either not be read by their addressees or might be misunderstood in terms of content.[204] Therefore, a wording similar to Art. 12(1) GDPR would be appropriate in Art. 3(2). It should oblige the contractual partners to provide the information in a short and meaningful way, for example by using icons, keywords or certificates[205] (comparable to Art. 42 et seq. GDPR). It would also be conceivable, for example, implementing an obligation to explain the lack of use of icons.[206]

Recently, the Council Presidency did include the use of URLs and QR codes to provide the information in Rec. 23.[207] When using these methods, however, it must be considered that many users will probably not call up the information at all out of convenience and thus will not receive it. Generally, the provision of information via such a "media breach" must therefore be assessed carefully.[208]

At best, a rule would be designed to encourage (of course only in digital environments) the use of electronic information delivery systems, such as PIMS[209] or privacy bots[210].[211] They offer the most effective way of tackling one's *information overload*.[212] For the development, establishment and implementation of PIMS or privacy bots, incentives must be created in

---

[202] Ebner, G., *ZD* 2022, 364 (367).

[203] Ebner, G., Weniger ist Mehr?, 2022, pp. 104 et seq.

[204] Cf. Gerpott, T., *CR* 2022, 271 (275); Ebner, G., Weniger ist Mehr?, 2022, pp. 111 et seq.

[205] Gerpott, T., *CR* 2022, 271 (275).

[206] Cf. Ebner, G., Weniger ist Mehr?, 2022, p. 321 pointing to § 161 German Stock Corporation Act (AktG).

[207] Council Presidency 2022/0047(COD) – 15035/22, p. 14.

[208] On the identical problem in the context of Art. 13 GDPR, see Ebner, G., Weniger ist Mehr?, 2022, pp. 151 et seq.

[209] For further information to PIMS see Efroni, Z. / Metzger, J. / Mischau, L. / Schirmbeck, M., Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing, *EDPL* 2019, 352 (357) f.; Specht-Riemenschneider, L. / Blankertz, A. / Sierek, P. / Schneider, R. / Knapp, J. / Henne, T., Die Datentreuhand, *MMR-Beil.* 2021, 25 (27); Kollmar, F. / El-Auwad, M., Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, *K&R* 2021, 73 (77) f.; Richter, F., Aus Sicht der Stiftung Datenschutz - "Der Einwilligungsassistent und die Chancen eines personal data ecosystem", *PinG* 2017, 122 (123); Kettner, S. / Thorun, C. / Vetter, M., Wege zur besseren Informiertheit, ConPolicy GmbH Institut für Verbraucherpolitik 2018, 83.

[210] For further information to privacy bots see Nüske, N. / Olenberger, C. / Rau, D. / Schmied, F., Privacy Bots - Digitale Helfer für mehr Transparenz im Internet, *DuD* 2019, 28 (29); Geminn, C. / Francis, L. / Herder, K., Die Informationspräsentation im Datenschutzrecht – Auf der Suche nach Lösungen, *ZD-Aktuell* 2021, 05335.

[211] Cf. Gerpott, T., *CR* 2022, 271 (275).

[212] Cf. Ebner, G., Weniger ist Mehr?, 2022, p. 137 et seq.

general, not just in the provisions of the Data Act. However, the establishment of PIMS is particularly useful in the context of the Data Act.[213]

The current design of Art. 3(2), however, will not lead to a significantly different presentation of information than under Art. 13 GDPR, at least in a visual respect. In order to avoid any confusion among the data subjects, it is important for the contracting parties to provide the information under Art. 3(2) explicitly separated from that under Art. 13 GDPR.[214] Nevertheless, it is to be expected that the "new" data (protection) notices will be equated by laypersons with those of Art. 13 and 14 GDPR and, at worst, perceived as equally annoying[215].[216] As with the existing privacy notices, there is a high risk of information overload and "click and forget"-behaviour.[217]

Rec. 23 underlines the "obligation to provide information does not affect the obligation for the controller to provide information to the data subject pursuant to Art. 12, 13 and 14 [GDPR]". Consequently, this means that the information of Art. 3(2) must be communicated in addition to that of Art. 13 GDPR.[218] Even if the relation to Regulation (EU) 2019/1150 (P2B-Regulation)[219] is not explicitly mentioned, it can be assumed that Art. 3(2) applies in addition to Art. 9(2) Regulation (EU) 2019/1150.[220]

The Different Informational Elements in Detail

Art. 3(2) specifies in eight letters several notices which must at least be communicated to the user before the conclusion of a corresponding contract. Using the words "at least" is not ideal as it leaves room for further unnamed information duties.[221] A corresponding formulation was also found in the Commission's proposal for the GDPR[222], which was fortunately deleted in the course of the legislative process.

According to Art. 3(2) (a) the user shall receive information regarding the nature and volume of the data likely to be generated by the use of the product or related service. With this basically useful information, the user can assess the intensity of data generation by the product or related service. The nature (or better: "type")[223] of the data can be easily presented (e.g. via icons) and divided into categories. When creating categories, it is important not to create categories that are too detailed, but also not too broad. The depth of detail of the categorisation is up to each contractual partner and depends on the type of data processing. The "volume" probably refers

---

[213] See in detail Ebner, G., *ZD* 2022, 364 (367).

[214] Ebner, G., *ZD* 2022, 364 (367).

[215] Cf. Roßnagel, A., Zukunftsfähigkeit der Datenschutzgrundverordnung, *DuD* 2016, 561 (563).

[216] Ebner, G., *ZD* 2022, 364 (367).

[217] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483); Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173); Ebner, G., *ZD* 2022, 364 (367).

[218] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483); Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174).

[219] Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services.

[220] Gerpott, T., *CR* 2022, 271 (275).

[221] See in detail Ebner, G., *ZD* 2022, 364 (368).

[222] Cf. Art. 14 GDPR in COM(2012) 11 final.

[223] The Council Presidency rightly proposes this change of wording, see Council Presidency 2022/0047(COD) – 13342/22, p. 40; ITRE PE732.704, p. 33.

to the amount of data that is likely to be generated. However, the determination of this will depend above all on the user's behaviour and might therefore be difficult to communicate (in advance). The amendment to include the "estimated volume"[224] makes sense in this respect, but is not absolutely necessary. Conceivable are abstract references to values within the scope of average use, which could be briefly described.[225] However, information about the format of the data and the collection frequency is with regard to the danger of information overload as well as Art. 3(2) (b) clearly not recommended.[226]

According to Art. 3(2) (b) the user shall be provided with the information whether the data is likely to be generated continuously and in real-time (cf. also Art. 4(1) Sentence 1). This information can be easily visualised with icons and allows conclusions about the volume of data generation. Since it will usually be known before a product is used whether the data will be generated continuously and in real time, the wording "likely to be" should be deleted.[227] Therefore, the reference to the volume of the data in lit. a could be deleted. [228] One might interpret the wording in such a way that information can be omitted if the data is generated neither continuously nor in real time. However, this would be contrary to the purpose and a correct understanding of the wording ("whether"). Therefore, it must also be stated that these practices do not occur.

According to Art. 3(2)(e) the user must be informed about how she or he may access the generated data. The explicit mentioning in Rec. 23 already indicates the high relevance of the right of access to data (Art. 4(1))[229] and the corresponding information. The information enables users to "access the access" of the generated data. It thereby provides and increases transparency for the users about what data is collected[230] and in which way it is accessible[231]. In this respect, it is necessary to provide an abstract reference to the existence of the right of access on the one hand and to its concrete execution on the other hand. For example, it would make sense to provide a brief reference and a link or QR-Code that leads to a corresponding portal of the contractual partner of the user.[232]

An additional *de-facto*-reference to the "data holder's data storage and retention policy"[233] does not make sense at least for cases within the scope of the GDPR, because this information is already provided via Art. 13(2)(a) GDPR. Incidentally, a reference to the storage period and the deletion concept should also be avoided, as the relevance in this respect is less high for non-personal data and unnecessarily threatens the risk of information overload.

---

[224] Council Presidency 2022/0047(COD) – 13342/22, p. 40; ITRE PE732.704, p. 33; LIBE PE737.389, p. 32.

[225] Ebner, G., *ZD* 2022, 364 (368).

[226] A different stand is taken by LIBE PE737.389, p. 32.

[227] Council Presidency 2022/0047(COD) – 13342/22, p. 40; ITRE PE732.704, p. 34.

[228] Ebner, G., *ZD* 2022, 364 (368).

[229] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1481) (1485).

[230] Rec. 23.

[231] Rec. 5.

[232] Ebner, G., *ZD* 2022, 364 (368).

[233] Council Presidency 2022/0047(COD) – 13342/22, p. 40.

According to Art. 3(2) (d) the user shall be provided with information whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used. The value of the reference to the intention to use by the manufacturer supplying the product or by the service provider remains unclear. In the event of an intended personal use of non-personal data (for example) by the seller, a separate data licence agreement with the user is required pursuant to Art. 4(6) Sentence 1. In this respect, the user might be aware of the contracting party's own use. A deletion of the information duty is therefore considered.[234]

In contrast, the fact that the data is passed on to third parties, just like the purposes of use, can have a decisive influence on the user's decision to conclude a contract. Therefore, they should be communicated in any case.[235] Insofar as the data generated is personal data, there may be duplications with Art. 13(1)(c) and (e) GDPR at the time of collection. However, since the data subject already received the relevant information due to Art. 3(2)(d), there could be no need to inform them again in accordance with Art. 13(4) GDPR. It should be noted, however, that unlike Art. 13(1)(e) GDPR, Art. 3(2)(d) does not require the naming of specific recipients or categories. In this respect, the information in Art. 13(1)(e) GDPR can have independent content in addition to Art. 3(2)(d).[236] If the contracting party is also the controller, it is advisable for the controller to already provide information about specific recipients or at least categories of recipients in the information pursuant to Art. 3(2)(d).

According to Art. 3(2)(e) the user shall receive information whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established. The data holder is defined in Art. 2(4) as a legal or natural person who has the right or obligation, in accordance with the Act, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data.[237]

Art. 3(2)(e) offers a corresponding two-step information system. First, information must be provided on whether the contracting party is the data holder. According to the wording of the article, information about the identity of the data controller only has to be provided separately if the contracting party is not the data holder.[238] This concept is not sufficiently convincing. The identity attributes described in the regulation are of utmost relevance for the user even if the contracting party is the data holder.[239] In this constellation, too, the user should be spared searching for the address of the data holder.[240] In this respect, the Council Presidency's amendment[241] is therefore very welcome.

---

[234] Also Ebner, G., *ZD* 2022, 364 (368).

[235] With corresponding proposal to amend the wording Council Presidency 2022/0047(COD) – 13342/22, p. 40; ITRE PE732.704, p. 34.

[236] Ebner, G., *ZD* 2022, 364 (368).

[237] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482).

[238] Ebner, G., *ZD* 2022, 364 (368).

[239] Ebner, G., *ZD* 2022, 364 (368).

[240] Ebner, G., *ZD* 2022, 364 (368).

[241] Council Presidency 2022/0047(COD) – 13342/22, p. 40.

Notices regarding the identity of the data holder contains information "such as its trading name and the geographical address at which it is established". At least in the context of Art. 13 GDPR, the opinion has now become established that the summonable address, consisting of (trade) name and geographical address, is the most important identity feature.[242] In order to prevent inconsistencies and attempts at circumvention, the "such as" should therefore be deleted.[243] For the rest, the identity must be described as precisely as possible.[244] Therefore, legal persons should be named with the legal form suffix and natural persons with their first name, surname and address.[245]

According to Art. 3(2)(f) the user must be aware of the means of communication which enable the user to contact the data holder quickly and communicate with the that data holder efficiently. Due to the close connection of the notices in Art. 3(2)(e) and lit. f, they could also have been combined in one paragraph. In the context of Art. 13(1)(a) GDPR, accessibility by telephone and electronic means have emerged as the most relevant contact options.[246] In this respect, telephone hotlines, online contact forms and e-mail addresses are ideal as "quick" and "effective" communication tools.[247]

According to Art. 3(2)(g) the user needs to know how he or she may request that the data are shared with a third-party. As in the case of lit. c, the user must be informed, on the one hand, about the abstract existence of the right to share data and, on the other hand, about its concrete exercise.[248] Practicable ways of dealing with both lit. c and lit. g have yet to emerge in practice. However, also in the context of lit. g, it is advisable to briefly explain the content of the right to share and then provide a link to a corresponding portal through which data share can be initiated.[249]

According to Art. 3(2)(h) the shall be informed about his or her right to lodge a complaint alleging a violation of the provisions of Chapter II with the competent authority referred to in Art. 31. As in the context of Art. 13(2)(d) GDPR, the current wording of lit. (g) raises the question of whether the regulation only requires information on the existence of the right to lodge a complaint or also the naming of a specific competent supervisory authority referred to in Art. 31.[250] Even if the Hungarian data protection authority made a contrary decision[251], it seems favourable that the contracting party does not have to designate a specific competent

---

[242] Cf. Ehmann/Selmayr/Knyrim, DS-GVO, 2nd ed. 2018, Art. 13 n. 34 „postalische Anschrift muss als Minimum wohl in jedem Fall genannt werden".

[243] Ebner, G., *ZD* 2022, 364 (368).

[244] At least for Art. 13 GDPR Article 29 Data Protection Working Party, WP 260 – Guidelines on transparency under Regulation 2016/679, 31.

[245] At least for Art. 13(1)(a) GDPR Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, DS-GVO, 2nd ed. 2020, Art. 13 n. 35.

[246] Article 29 Data Protection Working Party, WP 260 – Guidelines on transparency under Regulation 2016/679, 31; Paal/Pauly/Paal/Hennemann, DS-GVO BDSG, 3rd ed. 2021, Art. 13 n. 14.

[247] Ebner, G., *ZD* 2022, 364 (369); Ehmann/Selmayr/Knyrim, DS-GVO, 2nd ed. 2018, Art. 13 n. 34; Auernhammer/Eßer, DS-GVO, 7th ed. 2020, Art. 13 n. 24.

[248] Ebner, G., *ZD* 2022, 364 (369).

[249] Ebner, G., *ZD* 2022, 364 (369).

[250] Cf. Ebner, G., *ZD* 2022, 364 (369).

[251] The decision can be found at https://www.naih.hu/files/NAIH-2020-2000-hatarozat.pdf, see especially p. 8.

authority. This is already necessary because it will not always be possible to name a competent authority before the contract is being concluded.[252] Ultimately, the wording of lit. g can also be interpreted in such a way that the wording "with the competent authority referred to in Art. 31" is to be concluded in the actual notice.[253] The wording should definitely be improved, also because of the experience gained in the context of the GDPR.

Infringements

In the event of an infringement of Art. 3(2), the validity of the contract remains unaffected.[254]

Summary

Overall, it is to be welcomed that the information is basically limited to the most important pieces of information.[255] Only a few references could be deleted or improved. On the other hand, it would be desirable to clearly promote innovative mediation methods to facilitate the users' reception and understanding of the information. Icons and PIMS are particularly suitable for the information under Art. 3(2). They should therefore be included in the regulations and generally promoted.

Proposed Amendments:

Art. 3(1)

– Clarify that Art. 3(1) is a general principle and no enforceable obligation.

– The words "where relevant and appropriate" are to be deleted.

– Add the words "in a structured, commonly used and machine-readable format."

Art. 3(2)

– The words "at least" are to be deleted.

– Redraft Art. 3(2) in line with Art. 12(1) and (7) GDPR. It should oblige the contractual partners to provide the information in a short and meaningful way, for example by using icons or keywords.

– Redraft Art. 3(2) in a way that (in digital environments) the use of electronic information delivery systems (such as PIMS or bots) is encouraged.

– Consider an exception for c2c-relationships.

Art. 3(2)(a)

– The deletion of the reference to the volume of the data is to be considered.

Art. 3(2)(b)

[252] See already for Art. 13(2)(d) GDPR Bräutigam, P. / Schmidt-Wudy, F., *CR* 2015, 56 (61).

[253] Ebner, G., *ZD* 2022, 364 (369).

[254] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).

[255] Quite similar Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 85.

– "likely to be" is to be deleted.

Art. 3(2)(d)

– The deletion of "intends to use the data itself or" is to be considered.

Art. 3(2)(e)

– "whether the seller, the renter or lessor is the data holder and, if not," is to be deleted.

– "such as" is to be deleted.

3. User's Right of Access (Art. 4(1)-(5))

Right of Access

Art. 4(1) stipulates the Act's key instrument to the benefit of the user, a statutory right to access and to use data *generated by the user's use*[256] of a product or related service. The Council Presidency underlines:

> "Such data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular though facilitating the maintenance and repair of the products in question."[257]

If no direct access is possible (although Art. 3 points in that direction), the user has the right to claim access through Art. 4(1). This claim does not touch the technical 'rule' of the data holder, who still might be the only one being able to "access" the respective product. The user has no 'right' to take the access into his own hands by penetrating the IoT-product in a way not foreseen / opened by the data holder. Respectively, the Council Presidency proposes to introduce a new Art. 4(4a):

> "The user shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data."[258]

The data access is restricted by different rules – especially with regard to a data use with regard to competing products / competing markets in Art. 4(4).

It is highly debated whether and to what extent the data access right sets – from a Law & Economics perspective – functionally calibrated, sensible, and thought-through parameters and incentives.[259] Whilst it seems to be generally accepted that an information-only / transparency-

[256] See above for more details sub III. 2. and IV. 1.

[257] Council Presidency 2022/0047(COD) – 15035/22, p. 11.

[258] Council Presidency 2022/0047(COD) – 15035/22, p. 44.

[259] Cf. in this regard Kerber, W.,Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 8; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 212.

only approach (cf. Art. 3(2)) would not be sufficient[260], it is inter alia debated which kind of data shall be made accessible, especially with regard to 'raw data', 'prepared data', 'derived', 'inferred', and / or 'aggregated' data.[261] It is discussed whether the user activation the Data Act relies on will work in practise[262], whether collecting data sets from every user individually and not receiving bulk data is economically feasible and / or sensible – also with regard to SME.[263] It is considered whether sectoral approaches shall be favoured in opposition of the one size fits all-framework of the Data Act.[264] Additionally, it is doubted whether a general set of rules for B2B and B2C scenarios alike is appropriate.[265]

Use

The right encompasses according to the heading of Art. 4 access and use alike. It is rather unclear why the heading of the norm refers also to the "use" of data. Rec. 28 stipulates (that apparently next to Art. 5(1)):

> "The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so."

The notion of use implies that there might be scenarios where the user is not able to use the data after access (next to the explicit rule in Art. 4(4)). Especially, the "right" to use seems to contradict Art. 4(6) according to which the data holder's use of the data is dependent on a contractual agreement with (a 'licence' given by) the user. The term "and use" therefore only serves the clarification purpose that the user actually has – within the limits of Art. 4(4) – the right to use (but leaves room for unclarity with regard to the data licence agreement).[266]

The right seems to be – a first sight – under the condition that "data cannot be directly accessed by the user from the product". Rec. 21 points to "an on-device data storage or (…) a remote server to which the data are communicated. Access to the on-device data storage may be enabled via cable-based or wireless local area networks connected to a publicly available electronic communications service or a mobile network."[267]

---

[260] Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 10.

[261] Cf. in this regard Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 12 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 10 et seq. n. 20 et seq.

[262] Cf. e. g., Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956).

[263] Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 20 as well as Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 78, 100 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 9 n. 19.

[264] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 3 n. 3.

[265] Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p. 15.

[266] Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 7 n. 14.

[267] Rec. 21 continues: „The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder. They may be designed to permit the user or a third party to process the data on the product or on a computing instance of the manufacturer."

Mandatory Nature

From the general setting and from its framing as a statutory right, it is not surprising that Art. 4(1) is regarded as a mandatory right which the parties / the user and the data holder cannot contract away.[268] The mandatory nature has, however, seen criticism from inter alia an Economics perspective.[269]

The Council Presidency proposes to stipulate the mandatory nature explicitly in Art. 4(1a): "Any agreement between the data holder and the user shall not be binding when it narrows the access rights pursuant to paragraph 1."[270] It is, however, unclear why the Council Presidency proposes a respective para. 1a when at the same time a general rule on the mandatory nature of Chapter II is proposed.[271]

General Conditions

The right is targeted at personal and non-personal data alike (cf. Art. 2(1) and Rec. 31).

Access (and use) must be granted free of charge, without undue delay, and, if applicable[272], access (and use) must be granted continuously and in real-time.[273]

According to the Council Presidency additionally "easily, securely, in a structured, commonly used and machine-readable format and, where applicable, of the same quality as is available to the data holder".[274]

According to Art. 4(1) Sentence 2, the exercise of the right of Art. 4(1) is only dependent of „a simple request through electronic means where technically feasible ".

Data Scope and Data Quality

Rec. 31 – partly in the context of Art. 5(1) and in comparison to Art. 20 GDPR – spells out the scope of data encompassed:

> "It grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 [GDPR], this Regulation mandates and ensures the technical feasibility

---

[268] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 32 n. 81; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 217. Cf. also Specht-Riemenschneider, L., *MMR* 2022, 809 (820).

[269] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 219.

[270] Council Presidency 2022/0047(COD) – 15035/22, p. 44.

[271] Cf. below IV. 8 and Council Presidency 2022/0047(COD) – 15035/22, p. 47.

[272] Cf. in this regard Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 84.

[273] Cf. also Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 7.

[274] Council Presidency 2022/0047(COD) – 15035/22, p. 44. – also tackling criticism on the original proposal of Art. 4(1), cf. e. g., Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 7.

> of third party access for all types of data coming within its scope, whether personal or non-personal."

The Council Presidency underlines in Art. 4(1):

> "data (…) that are accessible readily available to the data holder, as well as the relevant metadata"[275]

The ITRE proposes to add:

> "Data shall be provided in the form in which they have been generated by the product, with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data."[276]

Rec. 28 points to the aspect of data quality:

> "The data holder should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the product or related service."

It remains unclear why Rec. 28 (only) refers to "data made available to the third party". The set standards of Rec. 28 do also apply to the access of the user as such. It is rather surprising that these standards (next to Art. 28) are only listed within a recital. One should consider to clarify these aspects on the article-level of the Act.

Identification of the User

Art. 4(2) tackles the question how the data holder knows whether the 'correct' user is requesting access. The data holder may only require information that is necessary to verify the user.

No information on the requested access shall be kept that is not "necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure" (Art. 4(2) Sentence 2).

Rec. 27 adds that "[i]n the case of personal data processed by a processor on behalf of the controller, the data holder should ensure that the access request is received and handled by the processor."

Specific Data Holder Duties

The Council Presidency proposes a new Art. 4(2a) (equivalent to Art. 5(4)) stipulating that "[t]he data holder shall not coerce, deceive or manipulate in any way the user or the data subject where the user is not a the data subject is not the user, by subverting or impairing the autonomy, decision-making or choices of the user or the data subject, including by means of a digital interface with the user or the data subject, to hinder the exercise of the user's rights [according to Art. 4]."[277]

Limits of the Right of Access I: Trade Secrets

---

[275] Council Presidency 2022/0047(COD) – 15035/22, p. 44.

[276] ITRE PE732.704, p. 35; cf. also p. 37 with regard Art. 5.

[277] Council Presidency 2022/0047(COD) – 15035/22, p. 44.

Whereas Rec. 30 generally points to the fact that "[a]ny trade secrets or intellectual property rights should be respected in handling the data", Art. 4(3) spells out that the fact the data requested are data holder's trade secrets is not as such a limit to the right of access. Art. 4(3) draws the line at "all specific necessary measures are taken to preserve the confidentiality", also and "in particular with respect to third parties".

However, the Art. 4(3) is formulated in a rather confusing way.[278] The norm implies that trade secrets *can* only be disclosed if respective measures are taken. This is, generally, not the case – as the data holder is free to grant access even without these measures (if he/she wants on a voluntary). The norm might be read in a way that access can be denied if "specific measures" are not available / suitable to preserve confidentiality. However, as Art. 4(3) Sentence 2 indicates – as a standard setting – a contractual agreement (non-disclosure agreement) between the data holder and the data user. Obviously, this further contractual layer adds (especially vis-à-vis consumers) to the complexity of the general contractual setting.[279]

The Council Presidency tries to tackle some of the aforementioned points by proposing as Art. 4(3):

> "Trade secrets shall only be disclosed provided that the data holder and the user take all necessary measures prior to the disclosure to preserve the confidentiality of trade secrets in particular with respect to third parties. Where such measures do not suffice, the data holder and the user shall agree on additional measures, such as technical and organisational measures, to preserve the confidentiality of the shared data, in particular in relation to third parties. The data holder shall identify the data which are protected as trade secrets."[280]

And as Rec. 28a:

> "(…) data holders can require the user or third parties of the user's choice to preserve the secrecy of data considered as trade secrets, including through technical means. Also, the data holders can require that the confidentiality of a disclosure must be ensured by the user and any third party of the user's choice. Data holders, however, cannot refuse a data access request under this Regulation on the basis of certain data considered as trade secrets, as this would undo the intended effects of this Regulation."[281]

Limits of the Right of Access II: Data Protection Law

A non-dispositive legal barrier to the right to access is set by Art. 4(5). The rule specifically focusses on the scenario where the user is not the data subject whose personal data is requested. According to the Council Presidency, "a valid legal basis under Article 6(1) [GDPR] and, where relevant, the conditions of Article 9 [GDPR] and Article 5(3) [ePrivacy-Directive] [must be] fulfilled."[282]

---

[278] Cf. for a discussion of Art. 4(3) in detail Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 86 et seq.

[279] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

[280] Council Presidency 2022/0047(COD) – 15035/22, p. 44.

[281] Council Presidency 2022/0047(COD) – 13342/22, p. 15.

[282] Council Presidency 2022/0047(COD) – 15035/22, pp. 45 et seq.

Rec. 24 confirms that data holders are considered to be a controller (Art. 4(7) GDPR) as far as personal data is processed

Access to personal data (Art. 4(1) GDPR) results in a transfer of data to the user – and therefore in a processing of personal data according to Art. 4(2) GDPR. From the negative formulation in Art. 4(5), it could be derived that for all other cases Art. 4(1) does provide a legal basis for this processing in the terms of Data Protection Law.[283] Consequentially, a respective transfer would not be dependent on legal justifications according to Art. 6(1)(a) and (f) GDPR or Art. 9 GDPR (with respect to special categories of data). The general debate during the legislative process, however, points to the opposite.[284]

Potentially and especially with respect to Art. 4(5), the Data Act will not "solve" the inherent tension between data and data protection law. The consequence of Art. 4(5) is of central significance for data holders. They must now find – a mission close-to-impossible – the 'correct' boundary between non-personal data and personal data. Not providing non-personal data (due to a 'wrong' classification as personal data) could now result in a fine (cf. Art. 33), Providing personal data in breach of Data Protection Law (due to a 'wrong' classification as non-personal data) could also result in a fine (cf. Art. 83 GDPR). Rec. 30 is at least of some assistance in this regard stating that "Processing of (…) data is subject to the rules established under [the GDPR], including where personal and non-personal data in a data set are inextricably linked."

Given the case of a natural person being the user open questions still remain when data of other natural persons than the user have been collected. These questions are tackled by Rec. 30:

> "The use of a product or related service may, in particular when the user is a natural person, generate data that relates to an identified or identifiable natural person (the data subject). (…) The data subject may be the user or another natural person. Personal data may only be requested by a controller or a data subject. (…) Under this Regulation, the user who is a natural person is further entitled to access all data generated by the product, personal and non-personal."

Art. 4(5) should mirror Rec. 30 and should clarify (at least) that where the user is a data subject, its request (Art. 4(1) Sentence 2) is considered to be a valid basis under Art. 6(1) and 9 of the GDPR with respect to its personal data.

In any case, Art. 4(5) requires users that are not a natural person (especially companies) to evaluate their (subsequent) processing of personal data according to Data Protection Law. As in particular Art. 6(1)(f) leaves enormous room for debate, processors will consider to collect consent declarations from the data subjects at stake. It is – from the outset however – unlikely that respective users will have (de facto) any chance to contact data subjects – consequently being dependent on the data holder's discretion (or the (financial) incentives set by the user in this regard) to 'intermediate' between data subjects and users.

Limits of the Subsequent Use by the User

Art. 4(4) tries to balance the data holder's and the user's interests – especially with regard to the data holder investments into a specific product. The rule stipulates a non-compete obligation

[283] Cf. Rec. 24.

[284] See in detail on the interplay with the GDPR above sub III. 2.

of the user. The user may not use the (personal or non-personal) data accessed (Art. 4(1)) "to develop a product that competes with the product from which the data originate." Apparently, the omission of 'related services' is no mistake, but result of a last-minute change to the Commission proposal.[285]

The vaguely formulated[286] rule has been criticised, especially, but not only, from an Economics perspective.[287] In addition, it is proposed to design Art. 4(4) as a non-mandatory rule.[288]

The consequences of a violation of Art. 4(4), however, are unclear.[289]

4. Data Licence Agreement; Use by the Data Holder (Art. 4(6))

Data Licence Agreement

Art. 4(6) Sentence 1 is a true (but slightly hidden) 'revolution' introduced by the Act.[290] The scope of the norm is limited to non-personal data (diverging from the general approach of the Act, but in order not to interfere with / to touch Data Protection Law) – and shares the reference point of the Art. 4(1)-(5) "generated by the use of a product or related service". The heavily debated and criticized[291] Art. 4(6) Sentence 1 stipulates that the data holder generally requires a contractual agreement with this user in order to use respective *non-personal* data.

Rec. 24 confirms and adds:

> "However, this Regulation (…) should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user."

The data licence agreement "may be part of the sale, rent or lease agreement relating to the product" (Rec. 24).

---

[285] Cf. Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482 fn. 57) with further references.

[286] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 88.

[287] Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 23 et seq.; Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 88 et seq.

[288] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 89.

[289] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

[290] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483) with further references. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 92: "crucial change".

[291] E. g., Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 92 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 19 et seq. n. 45 et seq.; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, pp. 215 et seq.

The Data Act does not provide specific contract law rules for the agreement according to Art. 4(6).[292] Different follow-on problems result from this fact.[293] It is, for example, unclear under which conditions the data licence agreement may be terminated.[294] Consequently, it is proposed to add a new Art. 4a to further specify this contractual relationship.[295]

It is another heavily debated question whether and in which setting users will actually negotiate and / or value the Art. 4(6)-agreement in practise.[296] There are strong concerns that the user will actually not be specifically aware of the agreement which might even be concluded implicitly.[297] On this basis, it is demanded to combine Art. 4(6) with a pairing prohibition to hinder a "Total-Buy-Out".[298]

De facto-Control by Agreement?

The (requirement of a) data licence agreement is not dependent on the right to access (and use) according to Art. 4(1) – or its exercise. Rather the requirement of an agreement comes along with the severe consequence that the data holder may not process non-personal data without a respective contractual agreement. This is a legal 'revolution' with regard to non-personal data. Art. 4(6) Sentence 1 leads to the surprising result that the processing of non-personal data is subject to stricter rules than the processing of personal data.[299]

More fundamentally, the requirement of a data licence agreement leads to a control option of the user – and therefore could be classified as an (contractual) "attribution" of non-personal data to the user.[300] Consequently, it is partly proposed to delete Art. 4(6) Sentence 1.[301] Despite the fact that the Data Act does not introduce any 'absolute' rights, this attribution requires a careful evaluation – also with regard to its economic consequences.[302]

It is generally – and beyond Art. 4(6) – heavily debated whether and to what extend the data access regime introduces and / or paves the way for some type of 'absolute' / 'IP-like' right

---

[292] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174).

[293] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 21 n. 52.

[294] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

[295] Specht-Riemenschneider, L., *MMR* 2022, 809 (820).

[296] Strong doubts by Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 93; Specht-Riemenschneider, L., *MMR* 2022, 809 (816 et seq.). Cf. also Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956).

[297] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 93.

[298] Specht-Riemenschneider, L., *MMR* 2022, 809 (817).

[299] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 20 n. 49; Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 216; Specht-Riemenschneider, L., *MMR* 2022, 809 (816).

[300] Specht-Riemenschneider, L., *MMR* 2022, 809 (818) takes a different stand and underlines the (still existing) technical-factual power domain of the data holder. Cf. also Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 19 n. 45.

[301] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 21 n. 53.

[302] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1486).

regarding non-personal data.[303] This debate has to be seen against the background that on the basis of the current law non-personal data (if one has access and notwithstanding trade secret law) can be used freely and without some form of consent and / or agreement by the 'producer'.

The access regulation proposed by the Data Act can be understood as to manifest the technical-factual 'rule' of the data holder who "only" might have to grant access to data "under his control".[304] To the same end, others do underline the co-generating of data by data holder and user.[305] Some commentators connect such a co-generation with the idea of a 'co-property' (*Miteigentum*) leading towards a general 'right' of both the data holder and the user to use the respective non-personal data.[306]

Unfair Terms Control

A data licence agreement is subject to the unfair terms control according to Art. 13. Thereby, the Proposal does not stipulate any further rules regarding the data licence agreement if a consumer is a user as Art. 13 does only apply to business-to-business scenarios.[307] The Commission apparently came to the surprising conclusion that the general rules on unfair terms are sufficient. This approach is highly disputed and currently under review in the legislative process.

However, Rec. 24 might be regarded as a "minimum line" in this regard (also in b2c-scenarios). Rec. 24 combines in a rather confusing way elements of Art. 3(2)[308] and substantial elements:

> "Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder."

Specific Limits of the Use of the Data Holder

According to Art. 4(6) Sentence 2 stipulates that the data holder's use is limited in specific scenarios in which the data holder might "derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active".

Rec. 25 points to cases that

---

[303] See in detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 19 et seq. n. 44 et seq.

[304] Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, pp. 5 et seq.;Specht-Riemenschneider, L., *MMR* 2022, 809 (818). Cf. also the proposal of a new Art. 4(4a) by Council Presidency 2022/0047(COD) – 15035/22, p. 44 in this regard.

[305] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 219; as well as Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 85 et seq., 93 et seq.

[306] Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 216. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 80.

[307] See below VI.

[308] See above IV. 2.

> "involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate ([e].g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner."[309]

The words "such data" in Art. 4(6) Sentence 2 indicate that the limitation (being placed in Sentence 2 of Art. 4(6)) is referring only to non-personal data covered by Art. 4(6). It is, however, unclear why Sentence 2 carves out personal data – as there might also be a risk to undermine the commercial position of the user.

Furthermore, having the different parallel norm of Art. 5(5) in mind, it is unclear whether the limitations set by Art. 4(6) Sentence 2 are subject to a disposal of the parties.[310]

Proposed Amendments:

Art. 4(1)

– Consider a deletion of "and use" (if so, also in the heading of Art. 4).

– Consider a new Sentence 2: "The data holder should ensure that the data made available is as accurate, complete, reliable, relevant and up-to-date."

– The current Sentence 2 shall then become Sentence 3.

Art. 4(5)

– Consider a redrafting: "~~Where the user is not a data subject, a~~Any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Art. 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Art. 9 of Regulation (EU) 2016/679 are fulfilled. *Where the user is a data subject, its request (Art. 4(1) Sentence 2) is considered to be a valid basis under Article 6(1) and 9 of Regulation (EU) 2016/679 with respect to the access to its personal data.*

Art. 4(6) Sentence 1

– Consider to introduce more detailed rules regarding the data licence agreement in business-to-business scenarios. Alternatively, consider to extent the scope of Art. 13 respectively.

Art. 4(6) Sentence 2

– It should be clarified that Sentence 2 does also cover personal data. Systematically (to be separated from the data licence agreement) the sentence should be placed in a new Art. 4(7) where the "such data" shall just read "data".

Art. 4(7) (new)

[309] Rec. 25 further states that "[t]he user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission."

[310] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

– *"The data holder shall not use data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active."*

5. Right to Share Data with Third Parties (Art. 5)

Right to Demand Access in Favour of Third Party

Art. 5(1) widens the user's options. The user has – next to or instead of an access according to Art. 4(1) – the right to demand access in favour of a third party, the data recipient (Art. 2(7)) – similar to Art. 20(2) GDPR (cf. also Art. 5(7)). The third party can set financial incentives in order to 'activate' the user respectively.[311] In this case, the third party faces potentially 'double pricing' with respect to the compensation to be paid to the data holder according to Art. 9(1).[312]

The data scope and the general conditions are similar to Art. 4(1).[313] The conditions of the access are regulated by Art. 8 and 9.[314]

The ITRE proposes to add in a new para. 1a:

> "The right under paragraph 1 shall not apply to data resulting from the use of a product or related service in the context of testing of other new products, substances or processes that are not yet placed on the market unless use by a third party is permitted by the agreement with the enterprise with whom the user agreed to use one of its products for testing of other new products, substances or processes."[315]

The access to the benefit of the third party is restricted by different rules – especially with regard to a data use with regard to competing products / competing markets (Art. 5(5) and 6(2)(e)) as well as with regard to gatekeepers according to the DMA (which are considered to be illegitimate as third-party recipients, Art. 5(2), 6(2)(d)).

It is highly debated whether and to what extent the access on the basis of Art. 5 is – from a Law & Economics perspective – functionally calibrated, sensible, and thought-through.[316] It is especially discussed whether the user activation will work in practise.

---

[311] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 15.

[312] See below V. 2. as well as Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21. Cf. also Specht-Riemenschneider, L., *MMR* 2022, 809 (823); Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 27 et seq. n. 69 et seq.

[313] Cf. above IV. 3. as well as Council Presidency 2022/0047(COD) – 15035/22, p. 45.

[314] See also the proposal by Council Presidency 2022/0047(COD) – 15035/22, p. 45.

[315] ITRE PE732.704, p.38.

[316] Cf. in this regard Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022.

It is also considered whether sectoral approaches shall be favoured in opposition of the one size fits all-framework.[317] Furthermore, it is questioned whether the exclusion of gatekeepers as third-party recipients is serving the innovation and the common wealth.[318]

Third Party

According to Rec. 29, third party may be (but are not limited to) "an enterprise, a research organisation or a not-for-profit organisation." Natural persons might also be data recipients, however, only if they are "acting for purposes which are related to [their] trade, business, craft or profession" (Art. 2(7)). Consumers therefore seem to be excluded from the definition.

The right to access of Art. 5(1) is not a right of the third party, but is dependent on the user's exercise. It therefore generally comes along with the same practical challenges (user activation) Art. 20 GDPR faces.[319] Consequently, doubts as to its effectiveness have been articulated.[320] At least, with non-consumer users in mind it seems likely that Art. 5(1) will be an "living" instrument. Furthermore, data intermediaries (Art. 10 DGA) might serve as a catalysator in this regard.[321] Whilst the Commission proposal was rather silent on the interplay with the DGA, the Council Presidency now rightly points to:

> "Data intermediation services [as regulated by Regulation (EU) 2022/868] may support users or third parties in establishing a commercial relation for any lawful purpose on the basis of data of products in scope of this Regulation e.g. by acting on behalf of a user. They could play an instrumental role in aggregating access to data from a large number of individual users so that big data analyses or machine learning can be facilitated, as long as such users remain in full control on whether to contribute their data to such aggregation and the commercial terms under which their data will be used."[322]

Art. 5(1) follows Art. 4(1) regarding the parameters for access ("undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time").

Art. 5(3) regulates in parallel to Art. 4(2) the provision of information.[323]

(Second) Data License Agreement

Exercising the right of access to the benefit of the third party goes along with a contractual agreement (a second data license agreement) between the user and the third party regarding the

---

[317] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 3 n. 3.

[318] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 25 et seq.

[319] Cf. also Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

[320] Kerber, W., Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, pp. 6 et seq.

[321] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484). See also the proposed amendment to Rec. 29 by Council Presidency 2022/0047(COD) – 15035/22, p. 16.

[322] Council Presidency 2022/0047(COD) – 15035/22, p. 16.

[323] Cf. also Rec. 34: "In line with the data minimisation principle, the third party should only access additional information that is necessary for the provision of the service requested by the user."

use of the data according to Art. 4(6)) (that might be accompanied by an NDA according to Art. 5(8) Sentence 2).[324]

Termination of Access

Art. 5 does not explicitly clear how access (and / or the data license agreement) can be terminated. Rec. 34, however, spells out that "[i]t should be as easy for the user to refuse or discontinue access by the third party to the data as it is for the user to authorise access."

Gatekeepers Not Eligible As Third Parties

Bearing one of goals of the Data Act in mind, breaking up data silos, the highly debated[325] Art. 5(2) stipulates that gatekeeper according to the DMA are not eligible third parties.

Furthermore, gatekeepers are not allowed to

— "solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1)" (Art. 5(2)(a))

— "solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article" (Art. 5(2)(b))

— "receive data from a user that the user has obtained pursuant to a request under Article 4(1)" (Art. 5(2)I)

Rec. 36 points to the Commission's motivation in this regard

> "Start-ups, small and medium-sized enterprises and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach. At the same time, a small number of very large companies have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. These companies include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and whom existing or new market operators are unable to challenge or contest."

The Council Presidency adds:

> "Such inclusion would also likely limit the benefits of the Data Act for the SMEs, linked to the fairness of the distribution of data value across market actors."[326]

[324] See also below.

[325] Cf., for example, IMCO, PE736.701, pp. 27 et seq. proposing to delete Art. 5(2) entirely; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 25 et seq. Positively, Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 34 n. 91.

[326] Council Presidency 2022/0047(COD) – 15035/22, p. 19.

Regarding other forms of use and access, it is important to note that gatekeepers still have the option to obtain data in other contexts. Rec. 36 in the version proposed by the Council Presidency stipulates:

> "The exclusion of designated gatekeepers from the scope of the access right under this Regulation means that they cannot receive data from the users and from third parties. It should not prevent these companies from obtaining and using the same data through other lawful means. Notably, it should continue to be possible for manufacturers to contractually agree with gatekeepers that data from products they manufacture can be used by a gatekeeper company. The access rights under Chapter II of the Data Act contribute to a wider choice of services for consumers. The limitation on granting access to gatekeepers would not exclude them from the market and prevent them from offering its services, as voluntary agreements between them and the data holders remain unaffected."[327]

Specific Data Holder Duties

Art. 5(5) stipulates – in parallel to Art. 4(6) Sentence 2 – that "[t]he data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active".

Rec. 29 confirms that "[i]n making the data available to the third party, the data holder should not abuse its position to seek a competitive advantage in markets where the data holder and third party may be in direct competition."

In addition to Art. 4(6) Sentence 2 (at least *expressis verbis*), Art. 5(5) opens up a possibility for an "opt-out" of the third party: "unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time."

Specific Third Party Duties

According to Art. 5(4), "[t]he third party shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data."

Trade Secrets

Trade secrets are covered in a similar way, but in more detail by Art. 5(8).

A disclosure must be "strictly necessary to fulfil the purpose agreed between the user and the third party". It is unclear from the outset how and why the data holder should be aware of the purpose in the first place. One might read into the norm that the user has the obligation to disclosure the purpose to the data holder. In addition, Art. 5(8) rightly seems to assume that there will always be – in line with Art. 8 – a contractual agreement (including a non-disclosure agreement) between data holder and data recipiant and therefore a point of contact to clarify the purpose.

[327] Council Presidency 2022/0047(COD) – 15035/22, p. 19.

Art. 5(8) Sentence 2 additionaly adds that this contractual agreement shall specify "the nature of the data as trade secrets and the measures for preserving the confidentiality".

However, the Council Presidency proposes to delete this sentence and to add "The data holder shall identify the data which are protected as trade secrets."[328] instead.

Data Protection Law

Data protection law-related issues[329] are covered by Art. 5(6), (7) and (9). Art. 5(7) confirms that the Data Act does not touch the exercise of rights of the data subject under the GDPR, especially Art. 20 GDPR[330]. Rec. 31 spells out in detail: "[Art. 5(1)] complements the right to receive and port personal data under Art. 20 [GDPR] in several ways."

Art. 5(9) (additionally) confirms that the right according to Art. 5(1) "shall not adversely affect data protection rights of others". The Council Presidency proposes to delete the norm.[331]

Art. 5(6) is drafted in parallel to Art. 4(5)[332]). However, in comparison of both norms and not understandable, "by the data holder" is missing in in Art. 5(6). This should be added.

6. Obligations of Third Parties (Art. 6)

Art. 6 spells out the obligations of the data recipients which receive data on the basis of Art. 5(1). These are partly linked to an agreement between the user and the data recipient (Art. 6(1) implicitly highlights the fact (or better: the necessity) of an agreement between user and data recipient); partly, the obligations are to be obliged independently of an / the agreement.

Non-Exclusivity

With or without an agreement, the data recipient shall not – according to Art. 6(2)(f) – "prevent the user (…) from making the data it receives available to other parties." Doubts from an Economics perspective have been brought forward whether and to what extent the non-exclusivity does set negative incentives for data brokers.[333]

Limited Use / Non-Compete

According to Art. 6(1), the data recipient may only use the data received (1) for the purposes and under the conditions agreed with the user and (2) subject to the rights of the data subject (Art. 12 et seq. GDPR) insofar as personal data are concerned.[334]

According to Art. 6(2)(b), the data recipient may not "use the data it receives for the profiling of natural persons (…) [Art. 4(4) GDPR], unless it is necessary to provide the service requested

---

[328] Council Presidency 2022/0047(COD) – 15035/22, p. 46.

[329] Cf. in detail above sub III. 2. and IV. 3.

[330] Cf. Rec. 31 for the debate about the exact scope of Art. 20 GDPR.

[331] Council Presidency 2022/0047(COD) – 15035/22, p. 46.

[332] See above IV. 3.

[333] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21.

[334] Rec. 33 is even narrower: "In order to prevent the exploitation of users third parties to whom data has been made available upon request of the user should only process the data for the purposes agreed with the user and (…) and share it with another third party only if this is necessary to provide the service requested by the user."

by the user". Rec. 35 seems to be even stricter when referring to "processing activities [that] are strictly necessary to provide the service requested by the user".[335]

According to the highly debated[336] Art. 6(2)(e), the data recipient may not "use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose". The data recipient is allowed to "to develop a [non-competing] new and innovative product or related service" (Rec. 35).

Data Intermediation Services As Third Parties

Rec. 35 highlights: "Where the third party is a provider of a data intermediation service within the meaning of [Art. 10 DGA], the safeguards for the data subject provided for by that Regulation apply."[337]

Passing-On of Data

According to Art. 6(2)(c), a passing-on / a making available of the data received by the data recipient is not allowed:

> "to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user"

The phrase "unless this is necessary to provide the service requested by the user" indicates that the user and the third party might also agree on a general passing-on to a third party, e. g., for a 'sale' of the data (if that is regarded as the 'necessary' element of the service agreed on).[338]

The Council Presidency proposes to add

> "provided that the other third parties take all necessary measures agreed between the data holder and the third party to preserve the confidentiality of trade secrets;"[339]

According to the highly debated[340] Art. 6(2)(d), a passing-on / a making available of the data received by the data recipient is not allowed:

> "to an undertaking providing core platform services for which one or more of such services have been designated as a [DMA-]gatekeeper (…)"

Rec. 36 also importantly points to the service provision in the benefit of the third party:

---

[335] Cf. also Council Presidency 2022/0047(COD) – 15035/22, p. 46 in this regard.

[336] Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 13 et seq., 23 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 35 n. 94.

[337] Cf. also now Council Presidency 2022/0047(COD) – 15035/22, p. 16.

[338] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 7 n. 14. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 98.

[339] Council Presidency 2022/0047(COD) – 15035/22, p. 46.

[340] Cf., for example, IMCO, PE736.701, p. 28 and Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 35 n. 94 – proposing to delete Art. 6(2)(d) entirely – and Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 14.

> "(…) [T]hird parties to whom data are made available at the request of the user may not make the data available to a designated gatekeeper. For instance, the third party may not sub-contract the service provision to a gatekeeper."

Deletion of Data

The data recipient shall further "delete the data when they are no longer necessary for the agreed purpose" (Art. 6(1)). Rec. 35 makes clear that this duty "complements the right to erasure of the data subject pursuant to [Art. 17 GDPR]."

Impairing Decision-making

According to Art. 6(2)(a), the data recipient may not "coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user". Rec. 34 is additionally pointing to the fact that

> "third parties should not rely on so-called dark patterns in designing their digital interfaces. Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them. These manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service, in a way that subverts and impairs their autonomy, decision-making and choice. Common and legitimate commercial practices that are in compliance with Union law should not in themselves be regarded as constituting dark patterns."

The Council Proposal clarifies that Art. 6(2)(a) shall also protect data subjects if those are the user in question.[341]

7. Exemption of Micro and Small Enterprises; Virtual Assistants (Art. 7)

Micro and Small Enterprises

Art. 7(1) stipulates that "the obligations of this Chapter [II] shall not apply to data generated by the use of products manufactured or related services provided by (…) micro or small enterprises". (Art. 2 Annex to Recommendation 2003/361/EC). It is required that these enterprises "do not have partner enterprises or linked enterprises" (Art. 3 Annex to Recommendation 2003/361/EC) "which do not qualify as a micro or small enterprise".

The exemption is rather unclear.[342] The norm may read in that way that micro and small enterprises shall not have the burden of the Art. 3-6. However, the norm does only point to the products and services itself (and not the enterprises). Furthermore, the exemption also seems to cover scenarios where bigger enterprises – as data holders – use the products / services of micro and small enterprises.

[341] Cf. Council Presidency 2022/0047(COD) – 15035/22, p. 46.

[342] A proposal to delete or at least to modify Art. 7 is made by Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 35 et seq. n. 96.

Rec. 37 sheds some light on this question. First, the enterprises do not have duties according to Art. 3(1)

> "Given the current state of technology, it is overly burdensome to impose further design obligations in relation to products manufactured or designed and related services provided by micro and small enterprises. That is not the case, however, where a micro or small enterprise is sub-contracted to manufacture or design a product. In such situations, the enterprise, which has sub-contracted to the micro or small enterprise, is able to compensate the sub-contractor appropriately."

Furthermore, respective enterprises do not fall under the personal scope of Art. 4 and 5 if they are manufacturer of a product or provider of a service. However, respective enterprises may be covered if the scenario as Rec. 37 spells out

> "A micro or small enterprise may nevertheless be subject to the requirements laid down by this Regulation as data holder, where it is not the manufacturer of the product or a provider of related services."

The Council Presidency proposes a new Art. 7(1) Sentence 2 in order to protect medium-sized enterprises in their R&D and market entry phase"[343]:

> "The same shall apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as medium-sized enterprises as defined in that same Recommendation, for either medium-sized enterprises that meet the threshold of that category for less than one year or that where it concerns products that a medium-sized enterprise has been placed on the market for less than one year."[344]

Virtual Assistants

Art. 7(2) clarifies that "[w]here [the Data Act] refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service." The Council Presidency proposes a respective Art. 1(2a), whilst deleting Art. 7(2) at the same time.[345]

Rec. 22 elaborates

> "Virtual assistants play an increasing role in digitising consumer environments and serve as an easy-to-use interface to play content, obtain information, or activate physical objects connected to the Internet of Things. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the Internet of Things, including those manufactured by other parties and can replace the use of manufacturer-provided interfaces such as touchscreens or smart phone apps. The user may wish to make available such data with third party manufacturers and enable novel smart home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual assistant's activation

[343] Council Presidency 2022/0047(COD) – 11194/22, p. 4. Cf. also Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 26.

[344] Council Presidency 2022/0047(COD) – 15035/22, pp. 47; cf. also the proposed amendment in Rec. 37 (p. 19).

[345] Council Presidency 2022/0047(COD) – 15035/22, pp. 39, 47.

> by the wake word and data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the product."

Rec. 22 further clarifies the data covered

> "(…) [O]nly the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation."

8. Mandatory Nature

The Council Presidency proposes a general rule in a new Art. 7(3) stipulating that

> "[a]ny contractual term which, to the detriment of the user, excludes the application of, derogates from or varies the effect of the user's rights under this Chapter shall not be binding on the user."[346]

A respective general rule is far from doubt; especially with regard to an Economics perspective.[347]

[346] Council Presidency 2022/0047(COD) – 15035/22, p. 47.

[347] Cf. also above IV. 3.

V. FRAND Obligations for Data Holders in Providing Access (Art. 8-12)

Chapter III ('Obligations for Data Holders Legally Obliged to Make Data Available', Art. 8-12) sets out general rules when complying with obligations to make data available, including – but not limited to – the mandates for data holders under Chapter II of the Proposal. Data is to be made available on fair, reasonable, and non-discriminatory (FRAND) terms as well as in a transparent manner. Amongst other things, a reasonable compensation must be agreed upon.

1. Conditions between Data Holder and Data Recipient

In case of a data access under Art. 5 or under other Union law or national legislation implementing Union law, Art. 8(1) sets out the principle of a **f**air, **r**easonable **a**nd **n**on-**d**iscriminatory access (FRAND). Rec. 5 also underlines the idea of encouraging fair data sharing practices. Rec. 38 (Rec. 38a of the Council Proposal[348]) clarifies that these general regulations do not apply to obligations regarding data access under the GDPR.

Already here, the indeterminacy of the scope of Chapter III is criticised, since the "provision of data to a data recipient" can fall under different legal acts of the EU, in particular the Digital Markets Act.[349] It is therefore proposed to clarify that Chapter III applies to obligations to make data available *only* where a reference to the Data Act is to be found.[350]

Rec. 39 states that "the parties should remain free to negotiate the precise conditions for making data available in their contracts, within the framework of the general access rules for making data available" and thus takes up the principle of contractual freedom. A favourable clarifying proposal proposes to change "of the general rules" to "laid out in this Regulation and the [DGA]".[351]

FRAND terms are an already known element in Competition Law and IP Law – and can also be found in Art. 6(11) Digital Markets Act.[352] The rather vague general FRAND conditions from Art. 8(1) initially offer the advantage of flexibility. Yet, it is argued that FRAND-law might not be a sensible solution in many cases covered by the Act.[353] It might prove to be difficult for law enforcers and courts to create general principles in order assess FRAND terms[354], starting by stating a definition for the term "fair", which is not provided by the proposal.[355]

---

[348] Council Presidency 2022/0047(COD) – 15035/22, p. 20.

[349] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 44 et seq.

[350] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 45. Cf. also for further proposals Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, p. 224 et seq.

[351] ITRE PE738.509, p. 132.

[352] Cf. Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 32.

[353] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 35.

[354] Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 36 et seq. n. 99; Metzger, A. / Schweitzer, H., *ZEuP* 2023, 42 (67 et seq.).

[355] vbw, Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 13.

It is questionable why Art. 8 addresses Art. 5 alone, since, even if the user receives access to the data "free of charge" according to Art. 4(1), the user should not receive the data on unfair, unreasonable or discriminatory terms.[356]

Rather by way of clarification, it was proposed by the Council Presidency to add the phrase "in business-to-business relations" to the wording of Art. 8(1), whereby consumer-related links will be excluded.[357]

Violation of Art. 13

According to Art. 8(2) a contractual term of an agreement must fulfil the conditions of Art 13, otherwise the term will not be binding on the parties.

The Draft Opinion of the Committee on the Internal Market and Consumer Protection (IMCO) proposes to expand the first sentence of Art. 8(2) to "A data holder shall not be liable for the data it [*lawfully*[358]] shares when the data is under control of the third party and shall agree with a data recipient the terms for making the data available".[359]

A clarifying proposal aims to delete the first sentence of Art. 8(2) and to change the wording of the second sentence to "Any contractual term concerning…".[360]

Another clarifying proposal of the Council Presidency is to add a half-sentence to the second sentence that states "…to the detriment of the user…".[361]

Prohibition of Discrimination

Art. 8(3), which is modelled on Art. 102 TFEU[362], states that a data holder is not allowed to discriminate comparable groups of data recipients (this formulation raises ambiguities[363]) as defined in Art. 3 of the Annex to Recommendation 2003/361/EC. When a data recipient asserts a term to be discriminatory, Art 8(3) states the duty of the data holder to demonstrate that there has been no discrimination. Rec. 41 adds:

> "In order to compensate for the lack of information on the conditions of different contracts, which makes it difficult for the data recipient to assess if the terms for making the data available are non-discriminatory, it should be on the data holder to demonstrate that a contractual term is not discriminatory. It is not unlawful discrimination, where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons. These obligations are without prejudice to Regulation (EU) 2016/679".

---

[356] Cf. Metzger, A. / Schweitzer, H., *ZEuP* 2023, 42 (67). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 22 n. 54.

[357] Council Presidency 2022/0047(COD) – 13342/22, p. 44; concurringly ITRE PE732.704, p. 40.

[358] The term „lawfully" is proposed by ITRE 738.548, p. 64.

[359] IMCO PE736.701, p. 28.

[360] ITRE PE738.548, p.65.

[361] Council Presidency 2022/0047(COD) – 15035/22, p. 48.

[362] Picht, Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022, 21.

[363] Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 15.

It is objected that the formulation of the FRAND concept as a unilateral obligation (of the data holder) could gain the risk of a superior standing of the data recipient.[364] This risk could be contained by reformulating the rule as mutual obligation of both parties, so private law courts and the dispute settlement bodies of Art. 10 could enforce the FRAND concept also against the data recipient where it is needed.[365]

In order to avoid an excessive and disproportionate burden on the data holder it was proposed to add the passage "the data holder shall without undue delay provide the data recipient with information showing that there has been no discrimination".[366] It remains questionable whether the passage achieves the intended purpose. In particular, the passage does not contain any further information on what specific information must be shared.

A generally welcomed suggestion is to insert the half sentence "that are comparable in terms of activity, size, type of business relationship".[367] This give more certainty to the data holder.

Exclusive Basis

According to Art. 8(4), there must be no data transfer between data holder and data recipient on an exclusive basis, unless requested by the user under Chapter II. This seems to be a reasonable approach in principle, as it promotes the exchangeability of data in a broader sense.[368]

However, Art. 8(4) could potentially affect current data license agreements already in force (and concluded before the enactment of the Act); such agreements often contain exclusivity clauses.[369]

One proposal seeks to delete the entire paragraph.[370]

More Information than Necessary

According to Art. 8(5), data holder and data recipient shall not provide more information than necessary to make sure the compliance of the agreed term or their obligations under the Data Act or other applicable Union law or national legislation implementing Union law.

It remains unclear whether Art. 8(5) only addresses the contractual parties as a data recipient (which is to assume) or also law enforcement or courts.[371]

Respect of Trade Secrets

---

[364] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 103.

[365] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n.103.

[366] Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 41.

[367] ITRE PE738.548, p.65 et seq.

[368] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

[369] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173).

[370] ITRE PE738.548, p.67; in favour of an adaptation of the wording cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 104.

[371] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 105.

The highly debated Art. 8(6) clarifies that an obligation to make data available to a data recipient must not result in a disclosure of trade secrets within the meaning of Directive (EU) 2016/943[372] unless otherwise provided by Union law, including the Data Act, or by national legislation implementing Union law.

It is criticised that Art. 8(6) could 'invite' data holders not to share data, arguing that otherwise trade secrets would be revealed.[373] Furthermore, Art. 8(6) seems to be incompatible with Art. 5(8).[374]

Partly, it is generally criticised that Art. 8(6) regulates the handling of trade secrets.[375] Therefore, this opinion proposes to delete Art. 8(6) completely.[376]

Specht-Riemenschneider has criticised the general priority of trade secrets in Art. 8(6) and Art. 5(8).[377] The protection of trade secrets could also be ensured by blacking out or pseudonymising sensitive data, without completely refraining the sharing of non-personal data.[378]

It is rightly proposed to harmonize Art. 4(3) and Art. 5(8) with Art. 8(6) in order to clarify that there is no obligation to share trade secrets with a data recipient except in the cases expressly provided by law.[379]

Proposed Amendments:

- The consequences of non-FRAND terms should be stated.[380]
- The relationship between FRAND-obligations and unfair terms (Art. 13) should be clarified.[381]

Art. 8

- The proposal by *Leistner/Antoin*e with regard to the scope of Art. 8 ("It should be clarified that such FRAND 'licenses' will also cover necessary and justified use acts in regard to trade secrets"[382]) should be considered.

[372] Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[373] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 106; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21.

[374] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 102 n. 284.

[375] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 102 n. 284.

[376] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 106.

[377] Specht-Riemenschneider, L., *MMR 2022*, 809 (821).

[378] Specht-Riemenschneider, L., *MMR* 2022, 809 (821).

[379] Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 41.

[380] See Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 21.

[381] See Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 21.

[382] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 101.

– The proposal by *Leistner/Antoine* to add further (partly optional) elements to Art. 8 ("Apart from the essential elements laid down in Art.8, other elements of FRAND agreements, such as e.g. cross-licenses, where appropriate, should be further analysed and, if necessary and appropriate, be added as additional optional elements to the catalogue of Art. 8 or be addressed in the Recitals"[383]) should be considered.

Art. 8(5)

– The wording of Art. 8(5) should additionally contain "… shall not be required to provide any information to each other".[384]

2. Compensations

Rec. 42 and Art. 9 underline the possibility of requesting reasonable compensation for making data available according to Art. 5 in connection with Art. 8. To avoid the compensation of Art. 9(1), the Data Act does not hinder the user to request the data free of charge according to Art. 4(1) by himself and then forward it on to third parties.[385] This 'easy way out' has been widely criticized.[386] The way is, however, only 'easy' if the user takes the technical burden – and has to technical capabilities – to access, store, and forward the respective data.

General

According to Art. 9(1) any compensation shall be reasonable. The difficulties to interpret the term "reasonable" are left to the dispute settlement bodies according to Art. 10.[387] It is especially argued from an Economics perspective that it will be very difficult to determine a respective compensation – and that corresponding lengthy negotiations and / or court proceedings are highly likely.[388] In order to counter-balance respective challenges, a rebuttable presumption of a zero-access price is proposed.[389]

In line with the proposed amendment to Art. 8(1), it was also proposed for Art. 9(1) to include the phrase "in business-to-business relations".[390]

[383] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 103.

[384] See Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 105.

[385] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (171).

[386] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 16 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 29 n. 72.

[387] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 37 n. 101.

[388] Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 15 et seq.

[389] See Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 24. Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 29 n. 72.

[390] Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 42.

There are many proposals to change the wording of Art. 9(1), especially to specify what the compensation consists of.[391] One of them is to amend the wording to

> "Any compensation agreed between a data holder and a data recipient for the costs incurred and investment required for making data available shall, in the case of non-personal data, be fair and reasonable, and strictly proportionate in the case of personal data".[392]

This suggestion specifies the rather vague wording of the Proposal and is therefore generally to be preferred. Another proposal is to add "Any compensation (…) shall not exceed the costs related to making the data available to the data recipient and which are attributable to the request".[393] This proposal suggests that "there is no point in creating any obstacles for users to share data with data recipients by allowing data holders to impose undue rents upon a legal obligation." The data holders "should be fully compensated for all relevant costs, not more than that".[394] Since this proposal incorporates the regulatory content of Art. 9(2) into Art. 9(1), it is consequently proposed to delete Art. 9(2).[395]

Micro, Small, And Medium-Sized Enterprises

Regarding micro, small or medium-sized enterprises, Art. 9(2) states that any compensation agreed shall not exceed the costs directly needed to make the data available to the data recipient and which are attributable to the request. Art. 8(3) shall apply accordingly.

Specht-Riemenschneider concludes from this that the compensations should not be understood as payment for the concrete data, in case of micro, small and medium-sized enterprises it should be understood as an actual "compensation" for the costs incurred and investment required for making the data available. [396]

The limitation set by Art. 9(2) can put large companies at a massive disadvantage and is consequently criticized on this ground.[397]

Furthermore, it can be asked why there is no further regulation for micro, small, or medium-sized enterprises acting as data holders.[398]

In order to actually limit the scope of Art. 9(2) to micro, small, or medium-sized enterprises alone, it is proposed to add the passage "provided those enterprises do not have partner enterprises or linked enterprises as defined in Art. 3 of the Annex to Recommendation 2003/361/EC which do not qualify as an SME".[399]

---

[391] Cf. ITRE PE739.548, p. 69 et seq.

[392] LIBE PE737.389, p. 46.

[393] ITRE PE738.548, p. 69 et seq.

[394] ITRE PE738.548, p. 70.

[395] ITRE PE738.548, p. 72.

[396] Specht-Riemenschneider, L., *MMR* 2022, 809 (822).

[397] BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 16.

[398] Vbw, Data Act, Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 18; Bitkom, 'Bitkom Position Paper EU Data Act Proposal' (19 April 2022), 2022, p. 6.

[399] Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 42.

Due to the increased relevance of data intermediaries in the supply of data, it is partially proposed to put data intermediaries in the area of compensations on the same level as SME.[400]

Costs According to Art. 9(2)

Rec. 45 defines direct costs as "are the costs necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production". Rec. 45 states further:

> "Direct costs for making data available should be limited to the share attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will have to be set up permanently by the data holder. Long-term arrangements between data holders and data recipients, for instance via a subscription model, could reduce the costs linked to making the data available in regular or repetitive transactions in a business relationship."

It is further proposed to add after the second sentence of Art. 9(2):

> "These costs include the costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection or production.". [401]

To extend the cost-based approach to any kind of data recipients one proposal is to change the wording of Art. 9(2) in "Any reasonable compensation (…)".[402]

Exclusion of Compensation

Art. 9(3) allows Union law or national legislation implementing Union law to exclude compensation for making data available or providing for lower compensation. Rec. 43 potentially sets up higher requirements for compensations, namely "the need to safeguard consumer participation and competition or to promote innovation in certain markets".

The ITRE Draft Report further proposes to delete Art. 9(3) in its entirety to ensure a coherent structure of the Data Act as a horizontal framework.[403]

Information

To ensure the compliance of compensation terms with the paras. 1 and 2, Art. 9(4) stipulates an obligation for the data holder to provide the data recipient with information containing the calculation of the compensation in a sufficient detailed form. Rec. 47 underlines the principle of transparency respectively.

While the Commission's draft spoke of the data recipient's possibility "to verify that the requirements of para. 1 and, where applicable, para. 2 are met" the Council Presidency proposes to use a more neutral wording that states the data recipient's possibility to "assess whether the requirements of…".[404]

Calculation

---

[400] MyData Global response of the Data Act, 2022, p. 5.

[401] Council Presidency 2022/0047(COD) – 13342/22, p. 45.

[402] ITRE PE739.548, p. 74.

[403] ITRE PE732.704, p. 42 et seq.

[404] Council Presidency 2022/0047(COD) – 15035/22, p. 49.

The abstract and vague wording "reasonable" of Art. 9(1) does generally not state a specific system of price setting, which makes it even more difficult to 'find' a respective compensation in dispute settlement scenarios or before courts.[405] A major hurdle in the calculation of the consideration is especially the "convertibility" of the data. The costs of collecting and transmitting the data are typically relatively low, while the collected data later have a high commercial value. [406] In this regard, it is considered whether a complete waiver or a flat-rate reimbursement in the amount of a few Euros would be more expedient than concrete calculation in individual cases, particularly in order to avoid the disruptive potential of concrete cost calculation.[407]

Another proposal is to create a new Art. 9(4a): "The Commission shall develop guidelines to determine what are the criteria for a reasonable compensation according to paragraph 1, set between data holders and data recipients".[408]

Furthermore neither Art. 9 nor Rec. 45 contains rules about the concrete calculation of the "costs related to making the data available to the data recipient and which are attributable to the request" mentioned in Art. 9(2).[409]

It could be argued that (4) does not provide a solid rule for law enforcers and courts to set any concrete standard of reasonableness.[410] In order to gather circumstantial evidence of reasonableness, *Podszun* proposes an obligation to file concluded contracts with an official body so that non-discrimination and reasonableness can be verified in individual cases.[411]

Proposed Amendment:

Art. 9(1)

– Include procedural guidance for the price / compensation negotiations.[412]

3. Dispute Settlement

Art. 10 regulates dispute settlement structures.

Rec. 48 points to "alternative ways of resolving domestic and cross-border disputes that arise in connection with making data available" to "strengthen trust in data sharing".

[405] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 104.

[406] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 52.

[407] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 54 et seq.

[408] ITRE PE739.548, p. 77.

[409] Gerpott, T., *CR* 2022, 271 (279).

[410] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 101 n. 280.

[411] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 53.

[412] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 104.

According to this provision, Art. 10(1) creates access to dispute settlement bodies, where disputes on the determination of fair, reasonable and non-discriminatory terms and conditions and on the transparent manner of data provision are to be resolved in accordance with Art. 8 and Art. 9. The dispute settlement body must apply for its authorisation in the respective member state. The criteria that the settlement body must fulfil in this respect are set out in Art. 10(2).

Rec. 48 states that when parties cannot agree on fair, reasonable and non-discriminatory terms, dispute settlement shall offer a "simple, fast and low-cost solution to the parties".

One may wonder why the possibility of dispute settlement is limited to FRAND-terms.[413] In view of this ambiguity, the Council Presidency has proposed to include Art. 13 in the FRAND test.[414]

It is further proposed to amend Art. 10(1) by adding the sentence "This is without prejudice to the data subjects' rights to seek redress before a supervisory authority, and to the controller's data protection obligations."[415]

Based on the consideration that an individual user has sometimes limited interest and / or capability to take action against unfair practices by certain companies, one might consider whether data recipients can claim on the behalf of the user. Consequently, it is proposed to introduce an Art. 10(1)(a) with the following wording:

> "The user shall have access to dispute settlement bodies, certified in accordance with paragraph 2 of this Article, to settle disputes with data holders or data recipients or any third party in relation to breach of user's rights under this Regulation. The user shall have the right to allow a third party to pursue its legal claims on its behalf."[416]

According to Art 10(2), the member state where the dispute settlement body is established should certify the body, at the request of that body. To become certified, the dispute settlement body has to demonstrate that it meets all of the following conditions:

> (a) it is impartial and independent, and it will issue its decisions in accordance with clear and fair rules of procedure;
>
> (b) it has the necessary expertise in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available, allowing the body to effectively determine those terms;
>
> (c) it is easily accessible through electronic communication technology;
>
> (d) it is capable of issuing its decisions in a swift, efficient and cost-effective manner and in at least one official language of the Union.

---

[413] Gerpott, T., *CR* 2022, 271 (279); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 40 n. 108; Cf. ITRE PE739.548, p. 79 with the propose to take in Art. 13 in the wording.

[414] Council Presidency 2022/0047(COD) – 15035/22, p. 49.

[415] LIBE PE737.389, p. 46.

[416] IMCO PE736.701, p. 29.

In case there is no certified dispute settlement body in a member state, at the date of application of the Data Act, that Member State should establish and certify a settlement body which fulfils the aforementioned conditions.

The Council Presidency proposes to add Art. 10(2)(a) pointing to "... non-discriminatory and fair rules of procedure".[417] It further proposes to extend the expertise mentioned in Art. 10(2)(b) to questions of compensation regarding Art. 9.[418]

With regard to Art. 10(2)(b), there is criticism that too little expertise exists on the subject of FRAND conditions in data access scenarios.[419] The provision also does not give concrete criteria. In addition, there is no or hardly any case law on this topic in the EU. Art. 10 also does not contain any requirements regarding the professional qualification of such settlement bodies.[420]

According to Art. 10(3) the certified dispute settlement bodies shall be notified to the Commission. The certified and notified dispute settlement bodies should be listed on a dedicated and updated website by the Commission.

Art. 10(4) regulates that parties shall be informed by the dispute settlement bodies about the fees, or the mechanisms used to determine the fees before the parties request a decision.

According to Art. 10(5) dispute settlement bodies must refuse a request to resolve a dispute, when the concerning dispute has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

It is criticised that Art. 10(5) does not regulate international jurisdiction, especially because Rec. 48 addresses this topic.[421] Rec. 48 and Rec. 49 are also rather brief and lay down more general rules. Concrete rules on international jurisdiction are not evident either from the Recitals or from Art. 10.

Art. 10 does not regulate the concrete competences of the settlement bodies. The right of one party to choose freely among the settlement bodies in the EU could lead to further conflicts, not at least because a party might prefer to start the conflict in the country of its domicile.[422] This again brings up the unanswered question of the application of Art. 4(1) Regulation (EU) 1215/2012 (Brussels I-bis Regulation)[423], which states the obligation to sue another party in the courts of the state of the defendant's domicile.[424]

However, even when Regulation (EU) 1215/2012 is applicable, there is a high chance that not all member states have certified settlement bodies, which raises the question, to which

---

[417] Council Presidency 2022/0047(COD) – 15035/22, p. 49.

[418] Council Presidency 2022/0047(COD) – 15035/22, p. 49.

[419] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 113.

[420] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 113.

[421] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 40 et seq. n. 111.

[422] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 40 et seq. n. 111.

[423] Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[424] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 40 et seq. n. 111.

settlement body a dispute should be brought.[425] In the end, the dispute would have to be brought before a private law court of the member state.[426]

Art. 10(6) states that the parties must be granted a reasonable period of time to demonstrate their point of view on matters the parties have brought before the settlement bodies. The parties shall also be provided with the submissions of the other party and any statement made by experts. In that context, the parties shall also be granted the possibility to comment on those submissions and statements.

It is proposed to add a new Art. 10(8a) that states:

> "Dispute settlement bodies shall be obliged, when dealing with personal data related disputes, to act in line with EU and national law in the field of personal data protection, including personal data protection case law."[427]

With a view to formal aspects, Art. 10(7) states that dispute settlement bodies shall hand down a decision within 90 days after the request for a decision has been made. Furthermore, the decisions shall be in writing or on a durable medium and must be supported by a statement of reasons supporting the decision.

According to Art. 10(8), the decision of the dispute settlement body only binds the parties if they have explicitly consented to its binding nature before the start of the dispute settlements proceedings. It appears questionable that Art. 10 does not provide for any possibility of enforcement before national courts, which leads to the conclusion that many disputes are not brought before a dispute resolution body in the first place.[428]

Rec. 50 stipulates that the parties shall not be prevented to exercise their fundamental rights to an effective remedy and to a fair trial. In this respect, Art. 10(9) states that Art. 10 does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State.

A welcomed proposal of the Council Presidency is to introduce a new Art. 10(7a) focusing on transparency and comparability of decisions of dispute settlement bodies, which reads as follows:

> "Dispute settlement bodies shall make publicly available annual activity reports. The annual report shall include in particular the following information:
>
> (a) the number of disputes received;
>
> (b) the outcomes of those disputes;
>
> (c) the average time taken to resolve the disputes;

[425] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 41 et seq. n. 112

[426] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 41 et seq. n. 112

[427] ITRE PE739.548, p. 80.

[428] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 114.

> (d) common problems that occur frequently and lead to disputes between the parties; such information may be accompanied by recommendations as to how such problems can be avoided or resolved, in order to facilitate the exchange of information and best practices."[429]

4. Technical Protection

To prevent unauthorised access to the data and to guarantee conformity with Art. 5, 6, 9, and 10 as well as with the agreed contractual terms for making data available, Art. 11(1) sets up the right of the data holder to apply appropriate technical protection measures, including smart contracts (cf. Art. 30). Nevertheless, such protection measures shall in particular not be used to hinder the user's right to effectively provide data to third parties in accord with Art. 5. The latter could be considered as the actual regulatory content of Art. 11.[430]

Technical protection measures are exempt from review by the dispute settlement bodies according to Art. 10.[431]

It is proposed to delete the passage "including smart contracts" and to add the sentence

> "Where personal data is concerned, these technical measures shall be consistent with the obligation of the data controller to implement appropriate technical and organizational measures so as to ensure a level of security appropriate to the risk of the personal data processing pursuant to data protection legislation."[432]

A different proposal is to include "encryption" and "metadata" to the wording of Art. 11(1).[433]

In order to enforce a no discrimination rule at the technical level as well, it is proposed to expand the second sentence of Art. 11(1) so that:

> "technical protection measures shall not be used as a means to discriminate between data recipients…"[434]

Another proposal is to add a third sentence to Art. 11(1) that states:

> "The third party shall upon the request of the user or the data holder provide with information on how the data has been used when there is a reasonable doubt for unlawful use or onward sharing of the received data."[435]

Art. 11(2) addresses the case in which a data recipient, for the purposes of obtaining data, provided inaccurate or false information to the data holder, used deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation.

---

[429] Council Presidency 2022/0047(COD) – 13342/22, p. 46 et seq.

[430] Specht-Riemenschneider, L., *MMR* 2022, 809 (823).

[431] Specht-Riemenschneider, L., *MMR* 2022, 809, (823).

[432] LIBE PE737.389, p. 47.

[433] ITRE PE739.548, p.82.

[434] Council Presidency 2022/0047(COD) – 13342/22, p. 47.

[435] ITRE PE739.548, p.81.

The proposal of the Council Presidency would like to include the development of a competing product in the sense of Art. 6(2)(e).[436]

Another proposal adds the phrase "or in the case of personal data, an appropriate legal basis" to Art. 11(2).[437]

In the aforementioned cases, the data recipient shall without undue delay, unless the data holder or the user instruct otherwise:

> (a) destroy the data made available by the data holder and any copies thereof;
>
> (b) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods.

It is proposed to add to Art. 11(2) a second sentence

> "Any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall not be binding on that party."[438]

A proposal in the ITRE Draft Report is to extend Art. 11(2)(b) by adding

> "inform the user of the unauthorised use or disclosure of data as well as the measures taken to put an end to the unauthorised use or disclosure of data".[439]

In addition, it is also proposed to add to Art. 11(2)(a)

> "The user has the same rights as the data owner and the data recipient the same obligations as those referred to in paragraph 2 of this article if the data recipient has violated the following provisions Art. 6, paragraph 2 (a) and (b)."[440]

It should also be noted that it is proposed to expand the wording of Art. 11(2) to include "incomplete" information and "for unauthorised purposes, including the development of a competing product within the meaning of Art. 6(2)(e) or disclosed" in order to strengthen the prevention of unauthorised use or disclosure of data.[441]

In order to equalise the rights of users and data holders, the Council Presidency proposes to introduce a new Art. 11(2a) with the following content:

> „Where the data recipient has acted in violation of Article 6(2)(a) and 6(2)(b), users shall have the same rights as data holders under paragraph 2."[442]

---

[436] Council Presidency 2022/0047(COD) – 13342/22, p. 47.

[437] LIBE PE737.389, p. 47.

[438] LIBE PE737.389, p. 48.

[439] ITRE PE732.704, p. 44.

[440] ITRE PE732.704, p. 45.

[441] ITRE PE732.704, p. 43.

[442] Council Presidency 2022/0047(COD) – 13342/22, p. 47.

Art. 11(3) clarifies that Art. 11(2)(b), shall not apply in either of the following cases:

> (a) use of the data has not caused significant harm to the data holder;
>
> (b) it would be disproportionate in light of the interests of the data holder.

The Council Presidency proposes to extend both cases regulated in Art. 11(3) by adding the wording "or the user".[443]

Art. 11 does not regulate the burdens of proof, the liability of the data recipient, or the form of his sanction.[444]

5. Scope of Obligations

Art. 12(1) states that the Chapter III applies when a data holder is obliged under Art. 5, or under Union law or national legislation implementing Union law (entering into force after the date of application of the Act, Art. 12(3)), to make data available to a data recipient.

Probably for reasons of clarification, the addition of the phrase "in business-to-business relations" is also proposed for Art. 12(1).[445] Also, changing the word "implement" to "adopted in accordance with" is proposed (again).[446]

It is proposed to add a new Art. 12(1a) that states:

> "The obligations set out in this Regulation do not preclude a reciprocity of data sharing between a data recipient, user and data holder agreed in contracts."[447]

According to Art. 12(2), whenever a term in a data sharing agreement excludes the application of this chapter, to the detriment of one party, or, where applicable, to the detriment of the user, this term shall not be binding on that party. The rules of Art. 8-11 DA are therefore conceived as (partially unilateral) mandatory law.[448]

To ensure the observance of the GDPR, one proposal is to add an Art. 12(2a) that states:

> "Any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall not be binding on that party."[449]

---

[443] Council Presidency 2022/0047(COD) – 15035/22, p. 51.

[444] Gerpott, T., *CR* 2022, 271 (279).

[445] Council Presidency 2022/0047(COD) – 13342/22, p. 48; ITRE PE732.704, p. 45.

[446] Council Presidency 2022/0047(COD) – 13342/22, p. 48.

[447] ITRE PE739.548, p.87.

[448] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1485).

[449] ITRE PE739.548, p.88.

VI. Unfair Terms for Data Access and Use between Enterprises (Art. 13)

Chapter IV ('Unfair Terms Related to Data Access and Use Between Enterprises', Art. 13) addresses unfair contractual terms in data sharing contracts between businesses, where unequal bargaining power might be used to impose unilaterally a contractual term on a micro enterprise or an SME (as defined in Art. 2 of the Annex to Recommendation 2003/361/EC).[450] If found to be unfair, such a term will not be binding.

Personal Scope

In accordance with the amendment objectives of Art. 9(2), it is also proposed here to amend Art. 13(1) by adding "provided those enterprises do not have partner enterprises or linked enterprises as defined in Art. 3 of the Annex to Recommendation 2003/361/EC which do not qualify as an SME...".[451]

It is discussed to extend the application of Art. 13 to all B2B-transactions. The Data Act proposal, however, assumes that there is no need for protection in contracts between large companies.[452]

It is heavily debated why the scope of application is limited to trade between companies,[453] hence why consumers are excluded from Art. 13.[454] The fact that Art. 13 does not apply to the benefit of consumers is partly explained by the already comprehensive protection provided by the law on general terms and conditions.[455] Rec. 26 also states that "in contracts between a data holder and a consumer as a user of a product or related service generating data, Directive 93/13/EEC applies to the terms of the contract to ensure that a consumer is not subject to unfair contractual terms".

Furthermore, it is questionable whether the unfairness test also applies if the imposing party is itself a micro, small or medium-sized enterprise, which raises the consequential question of the protective purpose of an unfairness test between two small companies.[456]

Another question is whether Art. 13 protects only data recipients or also data holders. The overall wording of the standard is neutral, whereas Art. 13(1) regulates the application to "remedies for the breach or the termination of data related obligations", which rather indicates an approach strictly related to data recipients.[457]

---

[450] Commission, COM(2022) 68 final Explanatory Memorandum, p. 15.

[451] Council Presidency 2022/0047(COD) – 13342/22, p. 48; ITRE PE732.704, p. 45.

[452] Staudenmeyer, D., *EuZW* 2022, 596 (600).

[453] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 47 n. 126, p. 48 n. 129.

[454] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 48 n. 129.

[455] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173).

[456] Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 14 et seq.

[457] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 47 n. 127.

In order to clarify this issue, one proposal wants to delete the micro, small or medium-sized enterprise-related passage of Art. 13(1) and aims to change the wording to "(…) imposed by one actor onto another shall not be binding on the latter actor if it is unfair".[458]

Rec. 52 underlines the importance of contractual freedom as an essential concept in B2B-relations. Rec. 52 states that not all contractual terms shall be subject to an unfairness test, but only to those terms "that are unilaterally imposed". In contrast, a term that is "simply provided by one party and accepted by the [SME] or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed".

It is to be emphasised that the concept of 'unilaterally imposed'-terms seems unrealistic in worldwide multi-party network contracts, which could lead to the necessity of the application of Art. 13 to multilateral agreements.[459]

Furthermore, it is criticised that the protection of companies in the area of data trading does not depend on the size of the company, but on the degree of data dependency, so a possible imbalance is not related to the size of a company.[460]

Unfairness

According to Art. 13(2), a contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.

Specific criteria for "good business practice" and a "gross deviation" from it remain unclear.[461] Also, it is questionable what the standard to define "good" business practice actually is.[462]

Regarding Art. 13(2), it is proposed to add a half-sentence, so the paragraph would state:

> "A contractual term is unfair it is of such a nature that objectively impairs the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial or non- commercial interest in the data in question, (…).".[463]

Clauses to Be Considered Unfair

To determine the unfairness of a clause, the criteria of Art. 13(3) serve as a "black (clauses) list".[464] Art. 13(4) is a "grey list".[465]

---

[458] ITRE PE739.548, p. 91 et seq.

[459] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 107.

[460] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 46 n. 125.

[461] BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 17 et seq.; Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 14.

[462] Cf. Staudenmeyer, D., *EuZW* 2022, 596 (599).

[463] ITRE PE739.548, p. 92.

[464] Gerpott, T., *CR* 2022, 271, 278; Staudenmeyer, D., *EuZW* 2022, 596 (598).

[465] Staudenmeyer, D., *EuZW* 2022, 596 (598).

Art. 13(3) states that a contractual term is unfair for the purposes of Art. 13 if its object or effect is to:

> (a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;
>
> (b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations;
>
> (c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

Despite setting up a standard of liability, Art. 13(3)(a) does not establish a reference for liability.[466]

Art. 13(4) defines that a term is presumed unfair for the purposes of Art. 13 if its object or effect is to:

> (a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;
>
> (b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;
>
> (c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;
>
> (d) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
>
> (e) enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.

Art. 13(4)(a) could be understood as a future ban on "as is"-clauses, which would lead to an obligation to contractually guarantee data quality.[467]

For reasons of clarification, it is proposed to add to Art. 13(4)(b) "(…) to the legitimate commercial or non-commercial interests of the other contracting party".[468]

---

[466] BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 18.

[467] Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173).

[468] ITRE PE739.548, p. 93.

Picking up the idea that users should be able to decide whether they are willing to "sell" data only to the contacting party, i.e. sharing data exclusively with the contracting party and getting a compensation for that, one proposal is to change and extend the wording of Art. 13(4)(c) to:

> „prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party, including data transmitted from a connected product, as defined under Article 3(2a), during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, extract, access or control such data or exploit the value of such data in a proportionate manner, unless it has presented that party with an explicit choice between concluding the agreement without limitation to its rights and the option to be compensated proportionately in exchange for foregoing those rights;".[469]

According to Art. 13(4)(d), a contractual term is presumed unfair if its object or effect is to:

> "prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed by that party during the period of the contract or within a reasonable period after the termination thereof;"

It is proposed to further refine the wording "copy of the data" – having the debate about the scope of Art. 15(3) GDPR in mind.[470]

A welcomed amendment is to add a new Art. 13(4)(e)(a) that states:

> "prevent the party upon whom the term has been unilaterally imposed from terminating the agreement within a reasonable time period".[471]

For Art. 13(3) and (4), it is suggested that the term "of this Article" be replaced by "of paragraph 2".[472]

The effectiveness of Art. 13(3) and (4) is doubted by some commentators.[473]

It is noteworthy that the cases regulated in Art. 13(3) have only a rudimentary reference to data such as Art. 13(3)(c), which speaks of the agreed data quality.[474] Further data reference is contained in Art. 13(4)(b), (c) and (d). In summary, the prohibitions on clauses are rather vague. The model contract terms provided for in Art. 34 by the Commission can and will be helpful in the interpretation of terms in the future.[475]

Unilaterally Imposed Term

Art. 13(5) states that a term shall be considered to be unilaterally imposed if it has been brought into the contract by one contracting party and the other contracting party has not been able to

---

[469] ITRE PE739.548, p. 94.

[470] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 108.

[471] ITRE PE739.548, p. 94.

[472] Council Presidency 2022/0047(COD) – 13342/22, pp. 48 et seq.

[473] Staudenmeyer, D., *EuZW* 2022, 596 (598).

[474] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1485).

[475] Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1485).

influence its content despite an attempt to negotiate it. Furthermore, the contracting party that supplied a contractual term has to demonstrate that the term has not been unilaterally imposed.

It is unclear how it would be possible for the imposing party to prove that the other party did not attempt to negotiate the terms.[476]

Moreover, the reference to "despite an attempt to negotiate it" in Art. 13(5) means that if a party accepts the conditions without resistance, it does not come within the scope and thus the benefit of Art. 13.[477] This does potentially counter-run to the goal to protect the legally less well-informed companies.[478]

Sanctions are considered if a data owner uses delaying tactics when negotiating the condition of access.[479]

Further Provisions

With the intention of sustaining the contract, Art. 13(6) clarifies that the remaining terms shall remain binding when the unfair contractual term is severable from the remaining terms of the contract.

Art. 13(7) clarifies that Art. 13 does not apply to contractual terms defining the main subject matter of the contract, i.e. those terms that define the specific performance[480] or determine the price to be paid.

The Council Presidency further clarifies: "This Article does not apply to contractual terms defining the main subject matter of the contract nor to the adequacy of the price, as against the data supplied in exchange."[481]

Staudenmeyer correctly points to the fact that no general transparency requirement is demanded (as known form unfair terms regulation) and that, consequently, there is no control of the main subject even if this subject is drafted in an opaque way.[482]

Rec. 53 states:

> "Furthermore, the rules on unfair contractual terms should only apply to those elements of a contract that are related to making data available that is contractual terms concerning the access to and use of data as well as liability or remedies for breach and termination of data related obligations. Other parts of the same contract, unrelated to making data available, should not be subject to the unfairness test laid down in this Regulation."

---

[476] Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 14.

[477] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 45 n. 122.

[478] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 45 n. 126; Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 56 et seq.

[479] Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 56.

[480] ECJ ECLI:EU:C:2014:282 = *EuZW* 2014, 506 – Kásler (C-26/13); CEJ ECLI:EU:C:2015:127 = *GRUR* Int. 2015, 471 – Matei (C-143/13).

[481] Council Presidency 2022/0047(COD) – 13342/22, p. 49.

[482] Staudenmeyer, D., *EuZW* 2022, 596 (602).

One proposal actually wants to delete the passage "or to contractual terms determining the price to be paid".[483]

According to Art. 13(8), the parties of a contract addressed by Art. 13(1) may not exclude the application of Art. 13, derogate from it, or vary its effects.

Furthermore, the conduction of market investigation to analyse new unfair business practices is considered.[484] A new Art. 13(8)(a) shall state:

> "Within 12 months from the entry into force of this Regulation, the Commission shall by means of implementing acts further develop guidelines on the reasonable prices for the compensation for data sharing and measures to prevent and mitigate data market distortion practices provided in Chapters III and IV".[485]

Scope of Application

Lastly it is to be mentioned that the Council Presidency proposes that "the provisions of Chapter IV shall apply to contracts concluded after (date of application of this Regulation)".[486]

Proposed Amendments:

- Consider of excluding scenarios where two micro, small or medium-sized enterprises are negotiating[487]
- Reconsider the application of Art. 13 to multilateral agreements[488]
- The Commission's non-binding model terms (Art. 34) shall not be included in the Art. 13-test, when imposed unilaterally[489]

Art. 13(4)

- The wording of Art. 13(4)(d) should be redefined (cf. Art. 15(3) GDPR).[490]

* * *

[483] ITRE PE739.548, p. 95.

[484] ITRE PE739.548, p. 97.

[485] ITRE PE739.548, p. 96.

[486] Council Presidency 2022/0047(COD) – 14019/22, p. 70.

[487] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 106.

[488] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 107.

[489] vbw – Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 14.

[490] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 108.

Version 1.0