IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU
Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES No. 22-07

THE DATA ACT

Article-by-Article Synopsis of the Commission Proposal

Moritz Hennemann / Gregor Lienemann

Version 1.0
March 2022

Place of Publication

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

Authors

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.

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).

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

Abstract

This publication systematizes the European Commission's Proposal for a Data Act. The text of the Proposal is presented in a structured form, along with the pertinent recitals and references to existing legislation. Where appropriate, the contents of the Proposal are outlined and briefly put into context. The resulting synopsis is meant to act as a first point of departure for further legal analysis and commentary on the Proposal as it evolves throughout the legislative process.

Cite as

Hennemann, M. / Lienemann, G. (2022). The Data Act – Article-by-Article Synopsis of the Commission Proposal. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-07*. Available at https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

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

Foreword

Dear Reader,

Since February 2022, the wider public and the Data Law community in particular has (finally) had the chance to have a look at the European Commission's Proposal for a Data Act. To assist this process, this publication systematizes the Proposal. The text of the Proposal is presented in a structured form, along with the pertinent recitals and references to existing legislation. Where appropriate, the contents of the Proposal are outlined and briefly put into context. The resulting synopsis is meant to act as (only) a first point of departure for further legal analysis and commentary on the Proposal as it evolves throughout the legislative process.

We are more than happy to hear your thoughts about this document 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 and / or gregor.lienemann@uni-passau.de.

We like to thank the entire team at the chair, first and foremost the student research assistant Johanna Heidbrink, for their extremely valuable support in the drafting process and for taking the burden of formatting this document.

Sincerely yours,
Moritz Hennemann & Gregor Lienemann

Contents

I. Introduction

On February 23 2022, the European Commission unveiled its long-awaited Proposal for a Data Act.[1] The Proposal introduces 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 in place.

This publication merges the Articles of the Proposal with the respective recitals, definitions, and with pending and enacted legislation that the Proposal makes reference to. In light of increasing legislative complexity (not only) emanating from the European Commission, a systematic view on the Data Act can hopefully contribute to a better understanding how this jigsaw piece fits with the broader strategic outlook and concomitant statutory instruments (e.g., the Data Governance Act and the Digital Markets Act). It may also be regarded as part of some *travaux préparatoires* for a dynamic commentary on the Data Act as it will take shape in legislative proceedings over the coming months.

Literature on the proposed Data Act:

Bomhard, D. / Merkle, M.	Der Entwurf des Data Act – Neue Spielregeln für die Data Economy, *RDi* 2022, 168
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)
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)
Hennemann, M. / Steinrötter, B.	Der Entwurf des Data Act, *NJW* 2022, forthcoming
Klink-Straub, J. / Straub, T.	Data Act als Rahmen für die gemeinsame Datennutzung *ZD-Aktuell* 2022, 01076

[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.

II. 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. Subject-matter (Art. 1 paras. 1 and 2)

Article 1

Subject matter and scope

1. This Regulation lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest:

2. This Regulation applies to:

(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.

Pertinent recitals: 4 (harmonised framework) – 5 (subject-matter) – 6 (general approach to data access and usage rights)

Pertinent definitions: data (Art. 2 no. 1) – product (Art. 2 no. 2) – related service (Art. 2 no. 3) – user (Art. 2 no. 5) – data holder (Art. 2 no. 6) – data recipient (Art. 2 no. 7) – public sector body (Art. 2 no. 9) – data processing service (Art. 2 no. 12)

2. Interplay with existing rules (Art. 1 paras. 3 and 4, Art. 35)

Article 1 (cont.)

3. Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU)

2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities. Insofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679.

4. This Regulation 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, including Regulation (EU) 2021/784 of the European Parliament and of the Council and the [e-evidence proposals [COM(2018) 225 and 226] once adopted, and international cooperation in that area. This Regulation shall not affect the collection, sharing, access to and use of data under 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 and Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying the transfer of funds. This Regulation shall not affect the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law.

Pertinent recitals: 7-8 (data protection and e-privacy) – 9 (consumer protection) – 10 (criminal proceedings) – 11-12 (product design and requirements) – 13 (public security)

Pertinent definitions: data (Art. 2 no. 1) – user (Art. 2 no. 5)

Laws cited (in order): General Data Protection Regulation (EU) 2016/679 – E-Privacy Directive 2002/258 EC – Regulation (EU) 2021/1784 on addressing the dissemination of terrorist content online – Money Laundering Directive (EU) 2015/849 – Funds Transfer Regulation (EU) 2015/847

Article 35

Databases containing certain data

In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the *sui generis* right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.

Pertinent recitals: 63 (conflict with public-sector access based on exceptional need) – 84 (no attribution of *sui generis* right to databases purely holding sensor data)

Pertinent definitions: data (Art. 2 no. 1) – product (Art. 2 no. 2) – related service (Art. 2 no. 3) – user (Art. 2 no. 5)

Law cited: Database Directive 96/9 EC

3. Definitions (Art. 2)

Article 2
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘data’ means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording;

(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 electronic communications service and whose primary function is not the storing and processing of data;

(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;

(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;

(5) ‘user’ means a natural or legal person that owns, rents or leases a product or receives a services;

(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;

(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;

(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;

(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;

(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);

(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;

(12) 'data processing service' means a digital service other than an online content service as defined in Article 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;

(13) 'service type' means a set of data processing services that share the same primary objective and basic data processing service model;

Law cited: Portability Regulation (EU) 2017/1228

III. 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) 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.[2] 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.[3] Conversely, limitations are placed on data holders and data recipients when it comes to (secondary) use of the data.

1. Prerequisites for data accessibility (Art. 3)

Article 3
Obligation to make data generated by the use of products or related services accessible

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.

2. Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format:

(a) the nature and volume of the data likely to be generated by the use of the product or related service;

(b) whether the data is likely to be generated continuously and in real-time;

(c) how the user may access those data;

(d) 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;

(e) 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;

(f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently;

(g) how the user may request that the data are shared with a third-party;

(h) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31.

Pertinent recitals: 4-6 (general approach to access and sharing rights for data stemming from the use of a product or related service) – 17 (scope of data generated by the use of a product or

[2] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 14.
[3] For further details cf Hennemann, M. / Steinrötter, B., Der Entwurf des Data Act, *NJW* 2022, forthcoming.

related service) – 19- 20 (accessibility by default, including for a plurality of users and by way of automatic execution) – 23 (obligation to provide information to the user)

Pertinent definitions: data (Art. 2 no. 1) – product (Art. 2 no. 2 with recitals 14-15) – related service (Art. 2 no. 3 with recital 16) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 no. 6)

2. User's right of access; licensed use by data holder (Art. 4)

Article 4

The right of users to access and use data generated by the use of products or related services

1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

2. The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.

3. Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.

4. The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate.

5. Where the user is not a data subject, 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 Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.

6. The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such 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.

Pertinent recitals: 21 (modalities of access – on-device or remotely)– 24 (contractual arrangement for manufacturer to use non-personal data) – 25 (complementary relationship with sector-specific data sharing instruments) – 27 (verification of user's entitlement to get access) – 28 (freedom of onwards usage, save for IP rights and the prohibition on developing competing products) - 30 (limitations for personal data; joint controllership of user and data holder)

Pertinent definitions: data (Art. 2 no.1) – product (Art. 2 no. 2, recitals 14-15) – related service (Art. 2 no. 3 with recital 16) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 no. 6)

Law cited: General Data Protection Regulation (EU) 2016/679

3. Right to share data with third parties for limited onwards use (Art. 5-6)

Article 5
Right to share data with third parties

1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without 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.

2. Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of [Regulation XXX on contestable and fair markets in the digital sector (Digital Markets Act), shall not be an eligible third party under this Article and therefore shall not:

(a) 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);

(b) 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;

(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).

3. The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.

4. The 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.

5. The 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, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.

6. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.

7. Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.

8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.

9. The right referred to in paragraph 1 shall not adversely affect data protection rights of others.

Pertinent recitals: 24 (no legal basis in itself under GDPR to provide access to a third party) – 28 (freedom of to share with third party offering aftermarket service) – 29 (identity of third parties; no anti-competitive behaviour on the part of data holder) – 31 (disclosure to third parties only upon user request; corollary to Art. 20 GDPR) – 36 (providers of core platform services / "gatekeepers" under the DMA barred from exercising access rights)

Pertinent definitions: data (Art. 2 no. 1) – product (Art. 2 no. 2 with recitals 14-15) – related service (Art. 2 no. 3 with recital 16) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 no. 6)

Laws cited (in order): Proposal for a Digital Markets Act (COM(2020) 842 final) – General Data Protection Regulation (EU) 2016/679

Article 6
Obligations of third parties receiving data at the request of the user

1. A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose.

2. The third party shall not:

(a) 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;

(b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is necessary to provide the service requested by the user;

(c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;

(d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article […] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)];

(e) 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;

(f) prevent the user, including through contractual commitments, from making the data it receives available to other parties.

Pertinent recitals: 32 (e-privacy directive for data held on terminal equipment) – 33/34 (purpose limitation / data minimisation for processing and further sharing by third parties; right to refuse access by users; no "dark patterns" employed by the third party) – 35 (corollary to Art. 17 GDPR; data intermediaries under the DGA as third parties)

Pertinent definitions: data (art. 2 no. 1) – product (art. 2 no. 2 with recitals 14-15) – user (art. 2 no. 5 with recital 18)

Laws cited (in order): General Data Protection Regulation (EU) 2016/679 – Proposal for a Digital Markets Act (COM(2020) 842 final)

4. Exemption of SMEs; virtual assistants (Art. 7)

Article 7

Scope of business to consumer and business to business data sharing obligations

1. The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise.

2. Where this Regulation 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.

Pertinent recitals: 22 (virtual assistants) – 36 (power imbalance between SMEs and "gatekeepers") – 37 (position of SMEs, including as sub-contractors and as data holders)

Pertinent definitions: data (Art. 2 no. 1) – product (Art. 2 no. 2 with recitals 14-15) – related service (Art. 2 no. 3 with recital 16) – virtual assistants (Art. 2 no. 4 with recital 22) – enterprise (Art. 2 no. 8)

Law cited: Recommendation 2003/361/EC

IV. 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.

Article 8
Conditions under which data holders make data available to data recipients

1. Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV.

2. A data holder shall agree with a data recipient the terms for making the data available. A contractual term concerning the access to and use of the data or the liability and remedies for the breach or the termination of data related obligations shall not be binding if it fulfils the conditions of Article 13 or if it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.

3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, it shall be for the data holder to demonstrate that there has been no discrimination.

4. A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.

5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law.

6. Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.

Pertinent recitals: 38 (FRAND conditions across different sectors; no restrictions imposed on voluntary data sharing)- 39 (freedom to contract specific conditions within the broader framework) – 40 (suggested contractual reference to basic rule on avoiding unfair contract terms) – 41 (reversed burden of proof regarding non-discriminatory nature)

Pertinent definitions: data (Art. 2 no. 1) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 no. 6) – data recipient (Art. 2 no. 7) – enterprise (Art. 2 no. 8)

Laws cited (in order): Recommendation 2003/361/EC – Trade Secrets Directive (EU) 2016/943

Article 9
Compensation for making data available

1. Any compensation agreed between a data holder and a data recipient for making data available shall be reasonable.

2. Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly.

3. This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.

4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.

Pertinent recitals: 42 (reasonable compensation, particularly for access-related costs) – 43 (regulated compensation for specific data types) – 44 (payment of compensation by SMEs not in excess of direct costs for making data available) – 45 (direct costs for making data available – definition) – 46 (minor leverage and negotiating balance in case of SME data holder) – 47 (transparent compensation by providing sufficiently detailed calculation information)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – data recipient (Art. 2 no. 7) – enterprise (Art. 2 no. 8)

Law cited: Recommendation 2003/361/EC

Article 10
Dispute settlement

1. Data holders and data recipients shall have access to dispute settlement bodies, certified in accordance with paragraph 2 of this Article, to settle disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available in accordance with Articles 8 and 9.

2. The Member State where the dispute settlement body is established shall, at the request of that body, certify the body, where the body has demonstrated 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.

If no dispute settlement body is certified in a Member State by [date of application of the Regulation], that Member State shall establish and certify a dispute settlement body that fulfils the conditions set out in points (a) to (d) of this paragraph.

3. Member States shall notify to the Commission the dispute settlement bodies certified in accordance with paragraph 2. The Commission shall publish a list of those bodies on a dedicated website and keep it updated.

4. Dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the parties concerned before those parties request a decision.

5. Dispute settlement bodies shall refuse to deal with a request to resolve a dispute that has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

6. Dispute settlement bodies shall grant the parties the possibility, within a reasonable period of time, to express their point of view on matters those parties have brought before those bodies. In that context, dispute settlement bodies shall provide those parties with the submissions of the other party and any statements made by experts. Those bodies shall grant the parties the possibility to comment on those submissions and statements.

7. Dispute settlement bodies shall issue their decision on matters referred to them no later than 90 days after the request for a decision has been made. Those decisions shall be in writing or on a durable medium and shall be supported by a statement of reasons supporting the decision.

8. The decision of the dispute settlement body shall only be binding on the parties if the parties have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings.

9. This Article does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State.

Pertinent recitals: 48 (simple, fast and low-cost dispute resolution) – 49 (right to reject pending dispute) – 50 (no prejudice to legal redress before Member State courts)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – data recipient (Art. 2 no. 7)

Article 11

Technical protection measures and provisions on unauthorised use or disclosure of data

1. The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1).

2. A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed 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 made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, 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.

3. Paragraph 2, point (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.

Pertinent definitions: data (Art. 2 no. 1) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 no. 6) – data recipient (Art. 2 no. 7) – smart contracts (Art. 2 no. 16)

Article 12
Scope of obligations for data holders legally obliged to make data available

1. This Chapter shall apply where a data holder is obliged under Article 5, or under Union law or national legislation implementing Union law, to make data available to a data recipient.

2. Any contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party.

3. This Chapter shall only apply in relation to obligations to make data available under Union law or national legislation implementing Union law, which enter into force after [date of application of the Regulation].

Pertinent definitions: data (Art. 2 no. 1) – user (Art. 2 no. 5 with recital 18) – data holder (Art. 2 Nr. 6) – data recipient (Art. 2 no. 7)

V. 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 unfairness of contractual terms in data sharing contracts between businesses, where unequal bargaining power has been exploited to unilaterally impose a contractual term on a micro, small or medium-sized enterprise (SME).[4] If found to be unfair, such a term will not be binding on the SME party to the contract.

Article 13
Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise

1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair.

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.

3. A contractual term is unfair for the purposes of this Article 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.

4. A contractual term is presumed unfair for the purposes of this Article 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;

[4] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 15.

(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.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.

6. Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding.

7. This Article does not apply to contractual terms defining the main subject matter of the contract or to contractual terms determining the price to be paid.

8. The parties to a contract covered by paragraph 1 may not exclude the application of this Article, derogate from it, or vary its effects.

Pertinent recitals: 26 (advance reference to Art. 13 para. 1 in conjunction with Directive 93/13/EC) – 51 (unfair terms not binding on SMEs due to contractual imbalance) – 52 (concept of unilateral imposition on SMEs – "take it or leave it") – 53 (unfairness test limited to parts of the contract concerning data sharing) – 54 (application to excessive terms, not to those of a merely commercially favourable nature) – 55 (application of general unfairness test in the absence of listed terms)

Pertinent definitions: data (Art. 2 no. 1) – enterprise (Art. 2 no. 8)

Laws cited (in order): Recommendation 2003/361/EC – Directive 93/13/EC

VI. Making data available to public-sector bodies based on exceptional need (Art. 14-22)

Chapter V ('Making Data Available to Public Sector Bodies and Union Institutions, Agencies or Bodies Based on Exceptional Need', Art. 14-22) creates a harmonised framework under which public-sector bodies may request certain data in specific scenarios, especially in the case of public emergencies such as public health emergencies or major natural or human-induced disasters.[5]

Article 14
Obligation to make data available based on exceptional need

1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.

2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.

Pertinent recital: 56 (need for data access in exceptional need, including for research purposes; exemption of SMEs)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 Nr. 6) – enterprise (Art. 2 no. 8) – public sector body (Art. 2 no. 9)

Law cited: Recommendation 2003/361/EC

Article 15
Exceptional need to use data

An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances:

(a) where the data requested is necessary to respond to a public emergency;

(b) where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency;

(c) where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and

(1) the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or

(2) obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.

[5] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 15.

Pertinent recitals: 57 (public emergencies) – 58 (equivalents to public emergency re prevention, recovery or public interest without any other recourse to obtain data)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – enterprise (Art. 2 no. 8) – public sector body (Art. 2 no. 9) – public emergency (Art. 2 no. 10 with recital 57)

Article 16
Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies

1. This Chapter shall not affect obligations laid down in Union or national law for the purposes of reporting, complying with information requests or demonstrating or verifying compliance with legal obligations.

2. The rights from this Chapter shall not be exercised by public sector bodies and Union institutions, agencies and bodies in order to carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. This Chapter does not affect the applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration.

Pertinent recitals: 59 (no pre-emption of voluntary private-public arrangements; no prejudice to reporting or compliance obligations) – 60 (criminal / administrative offences and penalties)

Article 17
Requests for data to be made available

1. Where requesting data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall:

(a) specify what data are required;

(b) demonstrate the exceptional need for which the data are requested;

(c) explain the purpose of the request, the intended use of the data requested, and the duration of that use;

(d) state the legal basis for requesting the data;

(e) specify the deadline by which the data are to be made available or within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request.

2. A request for data made pursuant to paragraph 1 of this Article shall:

(a) be expressed in clear, concise and plain language understandable to the data holder;

(b) be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested;

(c) respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available;

(d) concern, insofar as possible, non-personal data;

(e) inform the data holder of the penalties that shall be imposed pursuant to Article 33 by a competent authority referred to in Article 31 in the event of non-compliance with the request;

(f) be made publicly available online without undue delay.

3. A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024. Directive (EU) 2019/1024 shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.

4. Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body, in view of completing the tasks in Article 15 or to make the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. The obligations on public sector bodies, Union institutions, agencies or bodies pursuant to Article 19 apply.

Where a public sector body or a Union institution, agency or body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received.

Pertinent recitals: 61 (transparent and proportionate requests; "once-only principle") – 62 (inapplicability of Open Data Directive)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 no. 9)

Law cited: Open Data Directive (EU) 2019/1124

Article 18
Compliance with requests for data

1. A data holder receiving a request for access to data under this Chapter shall make the data available to the requesting public sector body or a Union institution, agency or body without undue delay.

2. Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request within 5 working days following the receipt of a request for the data necessary to respond to a public emergency and within 15 working days in other cases of exceptional need, on either of the following grounds:

(a) the data is unavailable;

(b) the request does not meet the conditions laid down in Article 17(1) and (2).

3. In case of a request for data necessary to respond to a public emergency, the data holder may also decline or seek modification of the request if the data holder already provided the requested data in response to previously submitted request for the same purpose by another public sector

body or Union institution agency or body and the data holder has not been notified of the destruction of the data pursuant to Article 19(1), point I.

4. If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.

5. Where compliance with the request to make data available to a public sector body or a Union institution, agency or body requires the disclosure of personal data, the data holder shall take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data.

6. Where the public sector body or the Union institution, agency or body wishes to challenge a data holder's refusal to provide the data requested, or to seek modification of the request, or where the data holder wishes to challenge the request, the matter shall be brought to the competent authority referred to in Article 31.

Pertinent recitals: 63 (possibility to decline or seek modification of request) – 64 (safeguards for personal data)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 no. 9) – public emergency (Art. 2 no. 10 with recital 57)

Article 19
Obligations of public sector bodies and Union institutions, agencies and bodies

1. A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 shall:

(a) not use the data in a manner incompatible with the purpose for which they were requested;

(b) implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects;

(c) destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data have been destroyed.

2. Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public sector body or the Union institution, agency or body shall take appropriate measures to preserve the confidentiality of those trade secrets.

Pertinent recitals: 65 (purpose-specific use; timely deletion) – 66 (confidentiality of data that disclose trade secrets)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 Nr. 9) – processing (Art. 2 no. 11)

Article 20
Compensation in cases of exceptional need

1. Data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge.

2. Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

Pertinent recital: 67 (reasonable compensation of data holder in cases other than public emergencies)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 no. 9) – public emergency (Art. 2 no. 10 with recital 57)

Article 21
Contribution of research organisations or statistical bodies in the context of exceptional needs

1. A public sector body or a Union institution, agency or body shall be entitled to share data received under this Chapter with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested, or to national statistical institutes and Eurostat for the compilation of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall act on a not-for-profit basis or in the context of a public-interest mission recognised in Union or Member State law. They shall not include organisations upon which commercial undertakings have a decisive influence or which could result in preferential access to the results of the research.

3. Individuals or organisations receiving the data pursuant to paragraph 1 shall comply with the provisions of Article 17(3) and Article 19.

4. Where a public sector body or a Union institution, agency or body transmits or makes data available under paragraph 1, it shall notify the data holder from whom the data was received.

Pertinent recital: 68 (authority to further share the data obtained with research organisations)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 no. 9)

Article 22
Mutual assistance and cross-border cooperation

1. Public sector bodies and Union institutions, agencies and bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.

2. Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested.

3. Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the competent authority of that Member State as referred to in Article 31, of that intention. This requirement shall also apply to requests by Union institutions, agencies and bodies.

4. After having been notified in accordance with paragraph 3, the relevant competent authority shall advise the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the relevant competent authority into account.

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – public sector body (Art. 2 no. 9)

VII. Switching between data processing services (Art. 23-26)

Chapter VI ('Switching Between Data Processing Services', Art. 23-26) introduces minimum regulatory requirements of contractual, commercial, and technical nature, imposed on providers of cloud, edge and other data processing services, to enable switching between such services. Where technically feasible, a minimum level of functionality for customers shall be preserved after switching to the new service.[6]

Article 23

Removing obstacles to effective switching between providers of data processing service

1. Providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:

(a) terminating, after a maximum notice period of 30 calendar days, the contractual agreement of the service;

(b) concluding new contractual agreements with a different provider of data processing services covering the same service type;

(c) porting its data, applications and other digital assets to another provider of data processing services;

(d) maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, in accordance with Article 26.

2. Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the original provider.

Pertinent recitals: 69 (facilitated switching as a remedy to barriers of market entry) – 70 (limited efficacy of self-regulatory frameworks, e.g. Free Flow of Non-Personal Data Regulation) – 71 (elaboration of data processing services; on-demand access / broad remote access to an elastic pool of distributed computing resources) – 72 (regulatory aim of contract switching and porting of digital assets; functional equivalence)

Pertinent definitions: data (Art. 2 no. 1) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12) – service type (Art. 2 no. 13) – functional equivalence (Art. 2 no. 14)

Article 24

Contractual terms concerning switching between providers of data processing services

1. The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services shall be clearly set out in a written

[6] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

contract. Without prejudice to Directive (EU) 2019/770, that contract shall include at least the following:

(a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing service or to port all data, applications and digital assets generated directly or indirectly by the customer to an on-premise system, in particular the establishment of a mandatory maximum transition period of 30 calendar days, during which the data processing service provider shall:

(1) assist and, where technically feasible, complete the switching process;

(2) ensure full continuity in the provision of the respective functions or services.

(b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;

(c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider, in accordance with paragraph 1, point (a) and paragraph 2.

2. Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period, which may not exceed 6 months. In accordance with paragraph 1 of this Article, full service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2).

Pertinent recitals: 73 (data processing services as customers) – 74 ("exit management"; assistance and support required to effectuate the switching process; no prejudice to GDPR and Digital Content Directive) – 75 (Cloud Rulebook and standard contractual clauses)

Pertinent definitions: data (Art. 2 no. 1) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12)

Law cited: Digital Content Directive (EU) 2019/770

Article 25
Gradual withdrawal of switching charges

1. From [date X+3yrs] onwards, providers of data processing services shall not impose any charges on the customer for the switching process.

2. From [date X, the date of entry into force of the Data Act] until [date X+3yrs], providers of data processing services may impose reduced charges on the customer for the switching process.

3. The charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned.

4. The Commission is empowered to adopt delegated acts in accordance with Article 38 to supplement this Regulation in order to introduce a monitoring mechanism for the Commission to monitor switching charges imposed by data processing service providers on the market to ensure that the withdrawal of switching charges as described in paragraph 1 of this Article will be attained in accordance with the deadline provided in the same paragraph.

Pertinent definitions: data (Art. 2 no. 1) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12)

Article 26
Technical aspects of switching

1. Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service.

2. For data processing services other than those covered by paragraph 1, providers of data processing services shall make open interfaces publicly available and free of charge.

3. For data processing services other than those covered by paragraph 1, providers of data processing services shall ensure compatibility with open interoperability specifications or European standards for interoperability that are identified in accordance with Article 29(5) of this Regulation.

4. Where the open interoperability specifications or European standards referred to in paragraph 3 do not exist for the service type concerned, the provider of data processing services shall, at the request of the customer, export all data generated or co-generated, including the relevant data formats and data structures, in a structured, commonly used and machine-readable format.

Pertinent recital: 76 (European standards for interoperability and open interoperability by way of delegated Commission legislation)

Pertinent definitions: data (Art. 2 no. 1) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12) – service type (Art. 2 no. 13) – functional equivalence (Art. 2 no. 14) – open interoperability (Art. 2 no 15) – interoperability (Art. 2 no. 19)

VIII. Transfer of non-personal data to third countries (Art. 27)

Chapter VII ('International Contexts Non-Personal Data Safeguards' [sic!], Art. 27) aims to prevent unlawful third-party access to non-personal data held in the Union by data processing services offered on the Union market through technical, legal, and organisational safeguards.[7]

Article 27

International access and transfer

1. Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.

2. Any decision or judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a provider of data processing services to transfer from or give access to non-personal data within the scope of this Regulation held in the Union may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State.

3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:

(a) where the third-country system requires the reasons and proportionality of the decision or judgement to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements;

(b) the reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third-country; and

(c) the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.

The addressee of the decision may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States.

The European Data Innovation Board established under Regulation [xxx – DGA] shall advise and assist the Commission in developing guidelines on the assessment of whether these conditions are met.

---

[7] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

4. If the conditions in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof.

5. The provider of data processing services shall inform the data holder about the existence of a request of an administrative authority in a third-country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

Pertinent recitals: 77 (conflicts of Union law with laws in third countries on access to non-personal data held within the Union; enforceability of access requests only in the presence of reasonability and proportionality tests as well as review processes) – 78 (prevention of unlawful access to non-personal data; technical safeguards, values and standards)

Pertinent definitions: data (Art. 2 no. 1) – data holder (Art. 2 no. 6) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12)

Law cited: Proposal for a Data Governance Act (COM(2020) 767 final)

IX. Interoperability (Art. 28-30)

Chapter VIII ('Interoperability', Art. 28-30) provides for essential requirements to be complied with regarding interoperability for operators of data spaces and data processing service providers as well as for essential requirements for smart contracts. Further technological convergence is envisioned through the proposed development of open interoperability specifications and European standards for the interoperability of data processing services.[8]

Article 28
Essential requirements regarding interoperability

1. Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services:

(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

(d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.

These requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements coming from other Union or national sectoral legislation.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 38 to supplement this Regulation by further specifying the essential requirements referred to in paragraph 1.

3. Operators of data spaces that meet the harmonised standards or parts thereof published by reference in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements referred to in paragraph 1 of this Article, to the extent those standards cover those requirements.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements under paragraph 1 of this Article

5. The Commission shall, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or in case it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary, with respect to any or all of the

[8] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

6. The Commission may adopt guidelines laying down interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission.

Pertinent recitals: 76 (European standards for interoperability and open interoperability by way of delegated Commission legislation) – 79 (semantic interoperability and core vocabulary developed by standardisation bodies)

Pertinent definitions: data (Art. 2 no. 1) – smart contracts (Art. 2 no. 16) – common specifications (Art. 2 no. 18) – interoperability (Art. 2 no. 19) – harmonised standard (Art. 2 no. 20)

Law cited: European Standardisation Regulation (EU) 1025/2012

Article 29
Interoperability for data processing services

1. Open interoperability specifications and European standards for the interoperability of data processing services shall:

(a) be performance oriented towards achieving interoperability between different data processing services that cover the same service type;

(b) enhance portability of digital assets between different data processing services that cover the same service type;

(c) guarantee, where technically feasible, functional equivalence between different data processing services that cover the same service type.

2. Open interoperability specifications and European standards for the interoperability of data processing services shall address:

(a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;

(b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;

(c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

3. Open interoperability specifications shall comply with paragraph 3 and 4 of Annex II of Regulation (EU) No 1025/2012.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft European standards applicable to specific service types of data processing services.

5. For the purposes of Article 26(3) of this Regulation, the Commission shall be empowered to adopt delegated acts, in accordance with Article 38, to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services in central Union standards repository for the interoperability of data processing services, where these satisfy the criteria specified in paragraph 1 and 2 of this Article.

Pertinent recital: 79 (semantic interoperability and core vocabulary developed by standardisation bodies)

Pertinent definitions: data (Art. 2 no. 1) – processing (Art. 2 no. 11) – data processing service (Art. 2 no. 12) – service type (Art. 2 no. 13) – functional equivalence (Art. 2 no. 14) – open interoperability (Art. 2 no. 15) interoperability (Art. 2 no. 19)

Law cited: European Standardisation Regulation (EU) 1025/2012

Article 30
Essential requirements regarding smart contracts for data sharing

1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements:

(a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

(b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

(c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

(d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers.

2. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements under paragraph 1 and, on the fulfilment of the requirements, issue an EU declaration of conformity.

3. By drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall be responsible for compliance with the requirements under paragraph 1.

4. A smart contract that meets the harmonised standards or the relevant parts thereof drawn up and published in the Official Journal of the European Union shall be presumed to be in

conformity with the essential requirements under paragraph 1 of this Article to the extent those standards cover those requirements.

5. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential the requirements under paragraph 1 of this Article.

6. Where harmonised standards referred to in paragraph 4 of this Article do not exist or where the Commission considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article in a cross-border context, the Commission may, by way of implementing acts, adopt common specifications in respect of the essential requirements set out in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Pertinent recital: 80 (interoperability and essential requirements for smart contracts)

Pertinent definitions: data (Art. 2 no. 1) – smart contracts (Art. 2 no. 16) – common specifications (Art. 2 no. 18) – harmonised standard (Art. 2 no. 20)

Law cited: European Standardisation Regulation (EU) 1025/2012

X. Implementation and Enforcement (Art. 31-34)

Chapter X ('Implementation and Enforcement', Art. 31-34) lays down the implementation and enforcement framework with regard to competent authorities in each Member State, including a complaints mechanism and co-operation with data protection authorities.[9]

Article 31
Competent authorities

1. Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation. Member States may establish one or more new authorities or rely on existing authorities.

2. Without prejudice to paragraph 1 of this Article:

(a) the independent supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to the processing of personal data;

(b) for specific sectoral data exchange issues related to the implementation of this Regulation, the competence of sectoral authorities shall be respected;

(c) the national competent authority responsible for the application and enforcement of Chapter VI of this Regulation shall have experience in the field of data and electronic communications services.

3. Member States shall ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of this Article are clearly defined and include:

(a) promoting awareness among users and entities falling within scope of this Regulation of the rights and obligations under this Regulation;

(b) handling complaints arising from alleged violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;

(c) conducting investigations into matters that concern the application of this Regulation, including on the basis of information received from another competent authority or other public authority;

(d) imposing, through administrative procedures, dissuasive financial penalties which may include periodic penalties and penalties with retroactive effect, or initiating legal proceedings for the imposition of fines;

(e) monitoring technological developments of relevance for the making available and use of data;

[9] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

(f) cooperating with competent authorities of other Member States to ensure the consistent application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;

(g) ensuring the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V;

(h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI are enforced consistently with other Union legislation and self-regulation applicable to providers of data processing service;

(i) ensuring that charges for the switching between providers of data processing services are withdrawn in accordance with Article 25.

4. Where a Member State designates more than one competent authority, the competent authorities shall, in the exercise of the tasks and powers assigned to them under paragraph 3 of this Article, cooperate with each other, including, as appropriate, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679, to ensure the consistent application of this Regulation. In such cases, relevant Member States shall designate a coordinating competent authority.

5. Member States shall communicate the name of the designated competent authorities and their respective tasks and powers and, where applicable, the name of the coordinating competent authority to the Commission. The Commission shall maintain a public register of those authorities.

6. When carrying out their tasks and exercising their powers in accordance with this Regulation, the competent authorities shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party.

Pertinent recital: 81 (competent authorities)

Law cited: General Data Protection Regulation (EU) 2016/679

Article 32
Right to lodge a complaint with a competent authority

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed.

2. The competent authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken.

3. Competent authorities shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay. This cooperation shall not affect the specific cooperation mechanism provided for by Chapters VI and VII of Regulation (EU) 2016/679.

Pertinent recital: 82 (right to lodge a complaint)

Law cited: General Data Protection Regulation (EU) 2016/679

Article 33
Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

2. Member States shall by [date of application of the Regulation] notify the Commission of those rules and measures and shall notify it without delay of any subsequent amendment affecting them.

3. For infringements of the obligations laid down in Chapter II, III and V of this Regulation, the supervisory authorities referred to in Article 51 of the Regulation (EU) 2016/679 may within their scope of competence impose administrative fines in line with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

4. For infringements of the obligations laid down in Chapter V of this Regulation, the supervisory authority referred to in Article 52 of Regulation (EU) 2018/1725 may impose within its scope of competence administrative fines in accordance with Article 66 of Regulation (EU) 2018/1725 up to the amount referred to in Article 66(3) of that Regulation.

Pertinent recital: 83 (penalties)

Laws cited (in order): General Data Protection Regulation (EU) 2016/679 – Regulation (EU) 2018/1725

Article 34
Model contractual terms

The Commission shall develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations.

Pertinent recitals: 83 (non-mandatory model contractual terms for b2b data sharing)

XI. Final Provisions (Art. 36-42)

Chapter XI ('Final Provisions', Art. 36-42) allows the Commission to adopt delegated acts on monitoring switching charges and further specifying standards for interoperability and smart contracts. In case standards are insufficient, implementing acts are permissible under the Proposal.[10]

Article 36
Amendment to Regulation (EU) No 2017/2394

In the Annex to Regulation (EU) No 2017/2394 the following point is added: '29. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]].'

Law cited: Consumer Protection Cooperation Regulation (EU) 2017/2394

Article 37
Amendment to Directive (EU) 2020/1828

In the Annex to Directive (EU) 2020/1828 the following point is added: '67. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]]'

Law cited: Directive (EU) 2020/1828

Article 38
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 25(4), 28(2) and 29(5) shall be conferred on the Commission for an indeterminate period of time from [...].

3. The delegation of power referred to in Articles 25(4), 28(2) and 29(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 25(4), 28(2) and 29(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council

[10] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Pertinent recital: 85 (delegated law-making under Art. 290 TFEU for certain aspects of the Proposal; interinstitutional agreement on the basis of Article 295 TFEU)

Article 39
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Pertinent recital: 86 (powers of the Commission to ensure uniform conditions for implementation)

Law cited: Regulation (EU) 182/2011

Article 40
Other Union legal acts governing rights and obligations on data and use

1. The specific obligations for the making available of data between businesses, between businesses and consumers, and on exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before [xx XXX xxx], and delegated or implementing acts based thereupon, shall remain unaffected.

2. This Regulation is without prejudice to Union legislation specifying, in light of the needs of a sector, a common European data space, or an area of public interest, further requirements, in particular in relation to:

(a) technical aspects of data access;

(b) limits on the rights of data holders to access or use certain data provided by users;

(c) aspects going beyond data access and use.

Pertinent recitals: 87 (Proposal without prejudice to sectoral rules and prior legislation on b2b, b2c, and b2g data sharing) – 88 (no restriction of competition contrary to Art. 101-102 TFEU intended by the Proposal)

Article 41
Evaluation and review

By *[two years after the date of application of this Regulation]*, the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee. That evaluation shall assess, in particular:

(a) other categories or types of data to be made accessible;

(b) the exclusion of certain categories of enterprises as beneficiaries under Article 5;

(c) other situations to be deemed as exceptional needs for the purpose of Article 15;

(d) changes in contractual practices of data processing service providers and whether this results in sufficient compliance with Article 24;

(e) diminution of charges imposed by data processing service providers for the switching process, in line with the gradual withdrawal of switching charges pursuant to Article 25.

Pertinent recital: 87 (evaluation by the Commission to ensure consistency and smooth functioning of the internal market)

Article 42
Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from *[12 months after the date of entry into force of this Regulation]*.

Pertinent recital: 89 (effective date)

* * *