Commission proposal (doc. 6596/22 – COM(2022) 68 final) **Deadline: 10 June 2022**

Data Act (Articles)

Important: In order to guarantee that your comments appear accurately, please do not modify the table format by adding/removing/adjusting/merging/splitting cells and rows. This would hinder the consolidation of your comments. When adding new provisions, please use the free rows provided for this purpose between the provisions. You can add multiple provisions in one row, if necessary, but do not add or remove rows. For drafting suggestions (2nd column), please copy the relevant sentence or sentences from a given paragraph or point into the second column and add or remove text. Please do not use track changes, but highlight your additions in yellow or use ~~strikethrough~~ to indicate deletions. You do not need to copy entire paragraphs or points to indicate your changes, copying and modifying the relevant sentences is sufficient. For comments on specific provisions, please insert your remarks in the 3rd column in the relevant row. If you wish to make general comments on the entire proposal, please do so in the row containing the title of the proposal (in the 3rd column).

Commission proposal	Drafting Suggestions	Comments
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)		General Scrutiny Reservation: The proposal needs further analysis and discussion. The following remarks are preliminary and without predjudice to further changes and amendments. Further remarks at a later date reserved. These remarks refer only to articles of the Data Act, not to recitals. Scrutiny Reservation: The difference of scopes between Data Act and General Data Protection Regulation (GDPR) needs further clarification and is currently being examined. Also being examined is whether further regulation within the Data Act (especially protection mechanisms for B2C relations) are necessary. In this context, we generally examine whether a clear

		differentiation between B2B and B2C is necessary. In the B2C context, we especially examine how the aim of the data act (ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data) can be best achieved taking into account the fundamental rights of protection of personal data, of freedom of science and of freedom to conduct a business. We furthermore ask for clarification if the Data Act already contains additional legal bases for processing personal data. The access of research organisations and researchers to privately held data (e.g. companies) should be strengthened with the Data Act. We are currently assessing, whether to for example include a new chapter on access to data for research organisations and researchers. The aim should be to ensure a level

		playing field in the European Union and a common European approach for the access to data for research organizations and researchers. The funding of research takes for the most part place on the European level, research consortia and alliances do research in the European single market – across national borders. Therefore common European rules are necessary. The access rights should be applicable to all fields of research and sectors, in other words shall cover research horizontally, that is why it is to be implemented in the Data Act. A concrete suggestion will follow.
CHAPTER I GENERAL PROVISIONS		
Article 1 Subject matter and scope		Not included is territorial scope for manufacturer of products and providers of services not established in the European Union

		(concerning non-personal data), e.g. as in Art. 3 GDPR: "Article 3 – Territorial scope 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

		3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.”
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.		
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	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, Regulation (EU) 2018/1725 and Directive 2002/58/EC, including the powers and competences of supervisory authorities.	See scrutiny reservation above on scopes of Data Act and GDPR.

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[1] 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	~~. 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[2] 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~~	Example for wording based on NIS 2 Directive.

[1] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).

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.	~~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.~~ 4. 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.~~ is without prejudice to the Member States' responsibilities to safeguard customs and tax administration and the health and safety of	

	citizens, public security, defence and national security or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order. 4a. This Directive does not apply to: (a) entities that fall outside the scope of Union law and in any event all entities that carry out activities in the areas of defence, national security, public security or law enforcement regardless of which entity is carrying out those activities and whether it is a public entity or a private entity; (b) entities that carry out activities in the areas of the judiciary, parliaments or central banks. Where public administration entities carry out activities in these areas only as part of their overall activities, they shall be excluded in their entirety from the scope of this Directive.	

	4b. This Directive does not apply to: (a) activities of entities which fall outside the scope of Union law and in any event all activities concerning national security or defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity; (b) activities of entities in the judiciary, the parliaments, central banks and in the area of public security, including public administration entities carrying out law enforcement activities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. 4c. The obligations laid down in this Directive do not entail the supply of information the disclosure of which is contrary to the Member	

	States' essential interests of national security, public security or defence. (4d) 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.	
	5. This Regulation does not affect Directive 93/13/EEC on Unfair Terms in Consumer Contracts.	Relationship to Directive 93/13/EEC should be clarified insofar as Articles 4 to 6 are dispositive.
	6. In so far as not regulated therein, this Directive shall not affect national general	Relationship to general contract law should be clarified.

	contract laws such as rules on formation, the validity or effects of contracts, including the consequences of the termination of a contract.	
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,	'product' means a tangible, movable item, including where incorporated in an immovable item, that are not primarily designed to display or play content, or to record and transmit	The workshops have demonstrated that the deviding line between devices that are covered (smartwatch) and that are not covered (smartphone) is still rather random. We

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;	content, 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;	therefore strongly suggest to provide a much clearer way of defining the products in scope. We welcome the EDPB and the EDPS recommendtion that the definition of "product" be amended so as to clearly exclude products such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners, also in the enacting terms of the Proposal (para. 42, EDPB/EDPS Joint Statement).
(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 performing one of its functions;		
(4) 'virtual assistants' means software that can process demands, tasks or questions	'virtual assistants' incorporated in or inter-connected with a product means software that	Is "software" sufficient or is "any combination of hard- and software" more precise?

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;	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 to 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;	'user' means a natural or legal person that owns, rents or leases a product or receives a related services;	Does "owns, rents or leases" cover all types of ownership of a product?
(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;		Clarification needed: - Why is the differentiation between "right or obligation" and "control of the technical design" needed ("or")? - Why is the differentiation between "in accordance with this Regulation, applicable Union law or national legislation implementing Union law" and "in case of non-personal data" needed ("or")?

		- Why are “non-personal data” and “through control of the technical design” linked (“and”)? - Could without altering the meaning Art. 2 (6) be worded: “‘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; We support the point made by the EDSA (para. 33 of the Joint Opnion) that, “the Proposal includes a different definition than the one found in the in the DGA for the term ‘data holder’, which may create legal uncertainty. Moreover, the definition of “data holder” in the Proposal should be further clarified.“

(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;		Does "trade, business, craft or profession" cover all purposes of data recipients? What about e.g. public sector bodies or data altruism organisations? Must a "data recipient always act for commercial purposes, etc.? What applies if a person is a third party within the meaning of Article 5? Does the third party also only fall under the definition , if he is acting commercially etc.?
(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	-'public sector body'	

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;	(9a) research organisation means an organisation as defined in Article 2 (1) of Directive (EU) 2019/790 of the European Parliament and of the Council";	
(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);		Should the definition of public emergency be limited to effects on the critical infrastructure of the Union, a Member State or part of it?

(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;	'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;	Art. 4 (2) defines "processing" without need for an "electronic format". Could become significant, if "making data available" is a category of "data processing" and if data is transferred in physical form (on a hard drive).
(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;		

	(12a) 'Customer' means someone who uses a data processing service, with or without paying for that service;	"customer" (in relation to Art. 23) should also be defined under Art. 2.
(13) 'service type' means a set of data processing services that share the same primary objective and basic data processing service model;		
(14) 'functional equivalence' means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract;		In order to allow competition of data procession services "functional equivalence" can only relate to services in the portfolio of the originating service and require "best effort".

(15) 'open interoperability specifications' mean ICT technical specifications, as defined in Regulation (EU) No 1025/2012, which are performance oriented towards achieving interoperability between data processing services;		
(16) 'smart contract' means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger;		Scrutiny Reservation: Are provisions concerning smart contracts (e.g. definition) necessary, or should smart contracts be defined in another horizontal legal act for more that data portability purposes. Furthermore are smart contracts needed in the context of the Data Act?
(17) 'electronic ledger' means an electronic ledger within the meaning of Article 3, point (53), of Regulation (EU) No 910/2014;		See scrutiny reservation above on smart contracts.

(18) 'common specifications' means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation;		
(19) 'interoperability' means the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions;	(19) 'interoperability' means the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange, understand and use data in order to perform their functions;	We suggest to supplement the definition of interoperability. The term "interoperability" can be understood in a multi-dimensional way. There is the organisational, semantic, syntactic and structural level of interoperability. All these levels contribute to achieving the aim of a full interoperability and have different, defined standards for this purpose. An important aspect of interoperability is that the data is understood (semantic level of interoperability). This shall be emphasized in the definition. Definition of data spaces needed, e.g. .”’data spaces' are a federated, open infrastructure for

		the sovereign access to and exchange of data based on common rules and standards for interoperability.“
(20) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012.		
CHAPTER II BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING		See above scrutiny reservation on the need for further analysis if more protection mechanisms in B2C relations are necessary.
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:	2. Before concluding a contract for the purchase, rent or lease of a product or a related service, the data holder shall at least provide the following information ~~shall be provided~~ to the user, in a clear and comprehensible format:	See EDPB/EDPS Joint Statement para. 48. Who shall provide the information. The vendor? The manufacturer of the product? Or the provider of the related service? It is necessary to clarify who has to meet the information requirements (manufacturer, seller/rentor/lessor or the data holder).
(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;	whether the data is ~~likely to be~~ generated continuously and in real-time;	More than likelihood needed for informing the user, possibly also information on time intervals of data tranfers.

(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;		In addition to manufacturer and service provider also obligation of data holder?
(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;		Also means of communication of manufacturer/service provider, if different from data holder?

(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.		
Article 4 The right of users to access and use data generated by the use of products or related services		We understand Article 4 to regulate a legal claim of the user against the data owner for access to the data. Our understanding of the Data Act's scheme is that Article 4 conclusively governs this claim. The user can rely solely on Article 4 Data Act when asserting the claim. Is it correct that Article 4 does not require an additional contractual agreement? This has not been made sufficiently clear so far. In the event that the parties voluntarily enter into an agreement:

		To what extent can Article 4, 5 and 6 be deviated from? A corresponding provision is missing.
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.	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, of the same quality as is available to the data holder and continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible. 1a. Any agreement between the data holder and the user shall not be binding when it narrows the access rights pursuant to paragraph 1.	Concerning "free of charge": Is there a need to include a provision to prevent misuse by the user (e.g. requesting several copies of the data) We suggest to include contractual safeguards for the relationship between the data holder and the user. Proposal means to address personal data, see above scrutiny reservation on scopes of Data Act and GDPR and on the need for further analysis if more protection mechanisms in B2C relations are necessary.

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.	3. Trade secrets shall only be disclosed provided that all specific necessary measures such as confidentiality agreements between the data holder and the user 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.	In Art. 2 (1) (c) of the TS-Directive 'trade secret' is defined as information that has been "subject to reasonable steps (…) to keep it secret". This means that the owner of a trade secret gets lost of the legal protection if the necessary steps to protect the trade secret are not taken. Therefore the data holder usually will be required to oblige the user to protect trade secrets contained in the data. Against this background we welcome the provision of Art. 4

		(3) sentence 1 of the Data Act that complements Art. 2 (1) (c) of the TS-Directive. However, we think that the agreement between the data holder and the user described in Art. 4 (3) sentence 2 is the normal and probably most common case to keep the information secret. We therefore recommend to clarify this by integrating sentence 1 into sentence 2. In any case, the relation between the Data Act and the TS-Directive should be clarified. It is pointed out in the Explanatory Memorandum, p 4, 2nd paragraph that the Data Act does not affect existing rules in the areas of intellectual property (except the application of the sui generis right of the Database Directive). How does this fit together with Art 3 (2) of the TS Directive stating the disclosure of a trade secret that is required or allowed by Union law is considered lawful under the TS-Directive? Does

		the TS Directive or the Data Act apply as lex specialis?
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.		Is this provision necessary? Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision? Also see above scrutiny reservation on scopes of Data Act and GDPR.
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		See above scrutiny reservation on scopes of Data Act and GDPR. The coherence of the requirements of Art. 4 Data Act on the

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.		processing of non-personal data for the data holder vis-à-vis the requirements of the GDPR for the controller of personal data needs further examination. Also manufacturer/service provider if different from data holder? Should power of data holder in the sense of Art. 7 (4) GDPR be further restricted, e.g.: "The performance of a contract, including the provision of a service, shall not be made conditional on a contractual agreement to process data that is not necessary for the performance of that contract."? We are scrutinizing whether in certain sectors such as agriculture requirements/specifications for the contractual agreement in Art. 4(6) should be implemented in Art. 4. This could be a compulsory minimum content of such a

		contractual agreement or certain clauses that shall not be used in such a contractual agreement. Though this is a central aspect, Art. 4 (6) leaves the content to the parties (except for Art. 13, which has a limited scope). We see that in certain sectors as in agriculture there is no symmetric bargaining power. Therefore safeguards should be implemented to ensure that users can obtain value from the co-generated data fully and to ensure the user's empowerment. This is relevant for constellations that do not fall within the scope of Art. 8 and 13. Also, Art. 8 and 13 do not foresee a minimum content of a contractual agreement.
Article 5 Right to share data with third parties		**Why has a different system been chosen for Article 5 than for Article 4?** -Article 5 can be read in such a way that Article 5 - like Article 4 - regulates a legal obligation to

		provide data, i.e. creates a comprehensive legal claim in favor of the data recipient (third party), which is not limited . in any way or made subject to a reservation, for example, of any contractual agreement that may have been reached. Moreover, this right to data access does not regulate any obligation to reimburse costs. Article 5 can therefore currently be read as meaning that data access can be based on Article 5 alone - and that a contractual agreement is not required. Article 5 raises the following question: 1) Why does Article 5 not – as in Article 4- also conclusively regulate the obligation of the data controller to transfer the data and/or give access to data to the third party? 2) - To what extent is a contractual agreement within the meaning of Article 8 required at all, if the data recipient can also assert data access,

		if necessary, by means of an action based solely on Article 5? 3) - Or should Article 5- contrary to the wording and system currently indicate - merely grant a right to enter into a contract for data access, with the data owner being able to determine the scope and conditions of access as long as the conditions are "fair. reasonable and non-discriminatory? However, this restriction, that it is precisely the right to conclude a contract and thus to access data to the extent that must necessarily be determined by contract, is not reflected in Article 5 itself. Such a regulatory approach also considerably restricts the right of access, as the data holder can determine the scope of access. **The connection between Article 8 and Article 5 is not sufficiently clear.**

		- In any case, it must be expressed more clearly in Article 5 and / or Article 8 to what extent the statutory claim exists and what the relationship is between this statutory claim and (additional / necessary) contractual agreements under Article 8. If Article 5 only grants the right to conclude a contract, this should also be clearly stated. - Provided that in Article 5 - similar to Article 4 - the scope of the statutory entitlement is made clearer, Article 8 could be limited to the regulations on deviation. **Use of data by third parties in the interest of the user** In our view, the distinction in Article 4 and Article 5 also does not take sufficient account of the fact that there are constellations in which the data are directly transferred to a third party with the consent of the user, but the data are to be used solely in the interest of the user, but, for

		example, from a technical point of view the user cannot exercise his right of access himself, but the data are used by the third party for troubleshooting or repair for the benefit of the user. How is it ensured that the compensation that the third party has to pay for the data access is not charged to the user?
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.		Can a "third party" also be a consumer, e.g. a hobbyist who repairs a product as a service? If "third party" can also be a consumer, how are the modalities of data provision regulated?
2. Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper,		See above scrutiny reservation on the need for further analysis if more protection mechanisms in B2C relations are necessary.

pursuant to Article […] of [Regulation XXX on contestable and fair markets in the digital sector (Digital Markets Act)[3]], 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;		

[3] OJ […].

(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).		Does this also concern data obtained according to the data portability rule of Art. 20 GDPR? See above scrutiny reservation on scopes of Data Act and GDPR.
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.		See above scrutiny reservation on scopes of Data Act and GDPR and on the need for further analysis if more protection mechanisms in B2C relations are necessary.
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		Is this provision necessary? Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision? See above scrutiny reservation on scopes of Data Act and GDPR.

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		What are the legal consequences if the data holder and the third party do not agree on a confidentiality agreement? Is the user required to refuse the disclosure of the data in this case?

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.	~~9. The right referred to in paragraph 1 shall not adversely affect data protection rights of others.~~	See above scrutiny reservation on scopes of Data Act and GDPR. We suggest to strike this provision as it offers no tangible additional protections. Where adversely effect are expected they should be addressed with specific provisions. Is this provision necessary? Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision? If that's the case should this provision with regard to Art. 1 (3) Data Act be erased?

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.		See above scrutiny reservation on scopes of Data Act and GDPR and see above scrutiny reservation on the need for further analysis of more protection mechanisms in B2C relations are necessary. Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision? ?
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;		See above scrutiny reservation on scopes of Data Act and GDPR. Is this provision in light of Art. 22 (2) GDPR necessary? Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision?
(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.		
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		What was the reasoning to exclude micro and small enterprises?

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.		
CHAPTER III OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE		

Article 8 Conditions under which data holders make data available to data recipients		See comments on Article 5 above; the relationship to Article 5 is not clear. In principle, Article 5 already gives the right to data access in full. Why is there a need for an additional contractual agreement? This would only lead to a restriction of the statutory right. Necessity of Article 8? Article 4 show that a statutory right to access data can be comprehensively regulated.The same could be achieved in Article 5. In order to protect SMEs, Aticle 5 could also be made mandatory if SMEs are involved. This would also eliminate the need for difficult contractual terms and further regulations for contractual agreements in Article 8.
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		Article 8 lays down conditions if "data holder is obliged to make data available to a data recipient under Article 5 or under other Union

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.		law or national legislation implementing Union law". For reasons of transparency, it should be specified here in concrete terms and as an enumeration which access rights are affected by Article 8. Such a concrete indication should also be necessary with regard to the assessment of the extent to which the legal act can be based on the authorization under 114 TFEU. The enumeration could be made directly in Article 8 or also by listing it in an annex to the Data Act. What does "reasonable" mean? To what extent is reasonable required in addition to "fair"? Does reasonable refer only to compensation? If it refers only to compensation, isn't Article 9 sufficient? Is data provision “not discriminatory” if Article 8(3) is complied with? Then the mention of

		non-discriminatory in Article 8(1) could be omitted. COM is kindly asked to present a list of "other Union law or national legislation implementing Union law" according to paragraph 1. Further analysis required if "other Union law or national legislation implementing Union law" according to paragraph 1 should be listed in an Annex 10.
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	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 is not fair[, not reasonable or disciminatory]. ~~fulfils the conditions of Article 13~~ or if it	It should be regulated in general, what applies if a contract condition is not fair, inappropriate or discriminatory. This should not only be regulated for contracts in which an SME is involved.

varies the effect of the user's rights under Chapter II.	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.		See above scrutiny reservation on scope of Data Act and GDPR.

		Is this provision necessary? Concerning personal data Regulation (EU) 2016/679 applies. Concerning non-personal data, according to Art. 4 (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.
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		Further analysis required if similar to Article 1(2) of Directive 93/13/EEC terms reflecting mandatory legislative or regulatory provisions and the provisions of the law of the European

data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.		Union or the law of the Member States or principles of international conventions to which the Member States or the European Union are parties should be exempt from the standard and scrutiny of Article 8(2).
Article 9 Compensation for making data available		The Data Act enables the reciprocity in the context of access to data, but may lead to an uneven level playing field in the context of the compensation. Even if Art. 9 (3) shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation, in reality this might lead to a situation where in the context of the PSD2 an institution has to provide the transaction data of the account free of costs, whereas the bank has to pay a compensation if it requires from the industry IoT-data of mobile devices. A consistent

		approach within the PSD2 review, open finance act as well as horizontal frameworks should be ensured. We suggest to give further guidelines on what might qualify a compensation as unreasonable in cases where the data concerned is personal data. (Also see above scrutiny reservation on scopes of Data Act and GDPR).
1. Any compensation agreed between a data holder and a data recipient for making data available shall be reasonable.		Lack of connection between Articles 5, 8 and 9. Article 5 implies the obligation to make data available. If a data recipient can simply invoke Article 5, why should he promise the data owner remuneration for this?
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	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	What about a data altruism organisation or a public body?

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.	costs directly related to making the data available t the data recipient and which are attributable to the request~~.~~; the data holder shall give the data recipient transparent information on the calculation of the costs directly related to making the data available.	Article 9(2) provides only for SMEs that the compensation may not exceed the cost of making the data available. What applies to cases in which data are made available to consumers other than users as third parties within the meaning of Article 5? Do third parties who are users not have to pay any compensation, or do they at least also have to comply with the limitation under Article 9(2)? Can a reasonable remuneration in individual cases also be lower than the remuneration regulated in Article 9(2)?
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.		Are there any examples of this?

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.		When is the compensation reasonable? What are the factors to be used to determine reasonableness when Article 9(2) does not apply?
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.		

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).		See above scrutiny reservation on smart contracts.
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;	erase ~~destroy~~ the data made available by the data holder and any copies thereof;	In conformity with definition of GDPR.
(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.		Should in the interest of proportionality another alternative be added, e.g. (c) pay for any damages incurred by the data holder and or the user of the product and or related service.
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].		
CHAPTER IV UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES		

Article 13 Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise	Article 13 Unfair contractual terms unilaterally imposed on ~~a micro, small or medium-sized~~ another 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.		Scrutiny reservation concerning scope and the general structure of Article 13. Inparticular the differentiation between SME and larger companies will create a conflict with the existing level of protection in DE. A specific proposal to further structure Article 13 will follow. It should be made clear in Article 13 that Article 13 only applies in the context of Article 8.
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;		
(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.		
CHAPTER V MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED		
Article 14 Obligation to make data available based on exceptional need		Scrutiny reservation: Further analysis needed in order to ensure a clear, predictable and precise legal framework for affected data holders while at the same time also taking into account the

		public sector' legitimate interests for access to data to fulfil their legal obligations.
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.		
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.		
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.		
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;		See above scrutiny reservation on scopes of Data Act and GDPR. Is this provision necessary? Is Regulation (EU) 2016/679 applicable on personal data regardless of this provision? If that's the case should this provision with regard to Art. 1 (3) Data Act be erased?
(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		We ask the Commission for written explanation how to deal with application for access to environmental data at any agency obtainend

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.		pursuant to this chapter. These data are much more open to the public than the ones covered by Directive 2019/1024. Basically, only with a very few exemptions we consider environmental data no matter where they are from accessable for the public as long as they are kept by any public sector body. Therefore we suggest the following amendment: “This Chapter shall not affect obligations of a public sector body laid down in Directive 2003/4/EC or corresponding national law regarding the access to environmental information.”
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.		
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 (c).	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 erasure ~~destruction~~ of the data pursuant to Article 19(1), point (c).	In conformity with definition of GDPR.
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		See above scrutiny reservation on scopes of Data Act and GDPR.

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.		Is this provision necessary? Is Art. 32 GDPR applicable on personal data regardless of this provision?
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.	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 may ~~shall~~ be brought to the competent authority referred to in Article 31.	Or in the interest of accelerating the process be brought directly before the courts.
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:	1. A public sector body or a Union institution, agency or body ~~having~~ who will receive~~d~~ 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;		See above scrutiny reservation on scopes of Data Act and GDPR. Is this provision necessary? Is Art. 32 GDPR applicable on personal data regardless of this provision?
(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.	erase ~~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 erased~~destroyed~~.	In conformity with definition of GDPR.

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.		
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.		
Article 21 Contribution of research organisations or statistical bodies in the context of exceptional needs	Article 21 Contribution of research organisations or **public bodies contributing to official public statistics** ~~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.	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 instituts~~ **to public bodies contributing to official public statistics** and Eurostat for the compilation of official statistics.	There are not only the statistical agencies but other agencies like environmental agencies in charge of statistical tasks. In the meaning of the act we would understand official and public statistics provided by national statistical agencies and other public authorities, too.
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.		
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.	Where a public sector body intends to request data from a data holder established in another Member State, it shall at the same time notify the competent authority of that Member State as referred to in Article 31, of that intention.	In the interest of accelerating mutual assistance and cross border cooperation.
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	After having been notified in accordance with paragraph 3, the relevant competent authority may ~~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	In the interest of accelerating mutual assistance and cross border cooperation.

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.	aim of reducing the administrative burden on the data holder in complying with the request.	
CHAPTER VI		
SWITCHING BETWEEN DATA PROCESSING SERVICES		
Article 23 Removing obstacles to effective switching between providers of data processing services		Any regulation on the switch of contracts should be aligned with DORA.
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	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:	is provided by a different service provider. In particular, providers of data processing services shall remove (…)	
(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;		Any regulation on the switch of contracts should be aligned with DORA.
(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.		
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 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).		
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.		
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.		
CHAPTER VII INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS		
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		Clarification of Commission's aim to not restrict international transfer but governmental access, pending the outcome of scheduled talks with COM on this chapter.

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.		
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.		
CHAPTER VIII INTEROPERABILITY		It has to be clarified if the duties from chapter 8 are also applicable to supervised companies and if so what would be the resulting obligations for the supervising authorities? In particular, in the financial sector detailed rules already exist. Hence, it needs to be clarified if the duties from the data act would apply on top of the existing rules, how the respective supervision would look like and it is essential that contradictions are avoided. If so this could also lead to doublication of the supervisory structure should be avoided which could result in gaps of supervision or unclea responsibilities.
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	(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;	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.		See above scrutiny reservation on smart contracts: Is provision concerning smart contracts necessary, or should smart contracts be regulated in another horizontal legal act for more that data portability purposes?
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 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	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.	data sharing, such as regarding rights to access and technical translation of consent or permission, taking into account inter alia the European Statistical System's (ESS), established by Regulation (EU) 223/2009 on European Statistics, implementation of Common European Data Spaces (CEDS).	
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.		
Article 30 Essential requirements regarding smart contracts for data sharing		See above scrutiny reservation on smart contracts.. Is provision for smart contract necessary, or should smart contracts be regulated in another horizontal legal act for more that data portability purposes? Also are Smart contracts

		necessary to reach the goals set out by Article 30? In addition to our comment under chapter 8: Smart contracts are defined in Art. 2 (16) as „computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger“. In the contect of electronic ledger reference is made to the current Art. 3 (53) 910/2014/EC. However, this definition is unclear as 910/2014/EC does not provide provisions in the context of electronic ledger. Only in the Com Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final) there is a definition: „Electronic

		ledger means a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering'". This definition of smart contracts results in a broad scope. This implies the risk that due to the wide definition of „Smart Contract" and „Electronic ledger" also conventional software as well as websites and portals of Banks and insurances companies will fall under the provision. Moreover, it remains unclear, who will be responsible according to the law: Whereas Art. 28 referes to the interoperationalisation: „Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services: … (d) the means to enable the interoperability of smart contracts

		within their services and activities shall be provided.“, it does not define „Operators of data spaces“. Art. 30 stipulates „Essential requirements regarding smart contracts for data sharing“, but without specifying the addresee: „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:…“ The indeterminated legal terms (in bold) leaves it unclear, who the obligator is and the concrete legal obligations of the supervisory authorities in relation to the entities under their supervision.
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).		
CHAPTER IX IMPLEMENTATION AND ENFORCEMENT		
Article 31 Competent authorities		Further assessment if an additional authority next to data protection bodies, competition bodies, network regulatory bodies, ordinary jurisdiction and dispute settlement bodies is needed. In any case cooperation mechanisms and distinction of competencies of the different bodies is necessary.
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:		Without prejudice on deciding the necessity of a Competent Authority: We suggest to lay down a mechanism to solve possible conflicts between the different authorities.
(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:		Without prejudice on deciding the necessity of a Competent Authority: We suggest to lay down coherent tasks and powers of the competent authorities for the member states to avoid difficulties and discrepancies regarding the inforcement. We are concerned that there could be the possibility of forum shopping.

(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;		
(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;		Without prejudice on deciding the necessity of a Competent Authority: We support Denmark's suggestion that a cooperation forum be established (DKOR 3.5.22)
(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	In such cases, relevant Member States may ~~shall~~ designate a coordinating competent authority.	Member states' souvereign competency

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.		
7. Member States shall ensure that the designated competent authorities are provided with the necessary resources to adequately carry out their tasks in accordance with this Regulation.		
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.		
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.		Without prejudice on decision of necessity of Competent Authority: We suggest to lay down coherent tasks and powers of the competent authorities for the member states to avoid difficulties and discrepancies regarding the inforcement. We are concerned that there could be the possibility of forum shopping.
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.		
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.		
CHAPTER X SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC		
Article 35 Databases containing certain data	Article 35 Derogation of the Sui-generis-right under Article 7 of Directive 96/9/EC ~~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	This Regulation takes precedence over the sui generis right provided for in Article 7 of Directive 96/9/EC. ~~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~~	Germany proposes to define more precisely the relationship between Data Act and Sui-generis-right under Article 7 of the Database Directive 96/9 by means of a lex-specialis-approach. This seems necessary in particular to adress the following substantial conflicts: - Article 35 Data Act in its drafted form (as an alleged clarification, cf Rec 84) only caters to

containing data obtained from or generated by the use of a product or a related service.	~~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.~~	databases containing raw data generated by IoT-Devices. However, protection under the sui generis right is also available where there are investments in verification and / or presentation of data, which is industry practice. This leads to an inheritent conflict between Data Act and Article 7(1) of Directive 96/9 and legal uncertainty. - The conflicting relationship between the emergency access right of the public sector provided for in Chapter V to databases covered by the sui generis right is currently not addressed in a legally binding manner (cf. Recital 63), which leads to considerable legal uncertainty. Corresponding Recitals 63 and 84 should be changed to reflect clearly that the Data Act is lex specialis to the sui generis right.

CHAPTER XI FINAL PROVISIONS		
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]].'		
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]]'		

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 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.		
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.		

Article 40 Other Union legal acts governing rights and obligations on data access 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.		It needs to be examined in more detail whether and to what extent (sector-) specific and complementary regulations on data access may be possible under Member State legislation.
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.		
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:	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. In addition to evaluating the effectiveness of this regulation in reaching the goals set out in the Commission's Initial Impact Assessment	

	Report t~~T~~hat evaluation shall also 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.		

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.		With regards to IoT products the date of the entry into force should be further clarified. According to COM rules are applicable for products newly placed on the market. In order to fulfil design obligations a longer transition phase is needed.
It shall apply from [12 months after the date of entry into force of this Regulation].		
Done at Brussels,		
For the European Parliament For the Council		
The President The President		

	End	**End**