Council of the European Union
General Secretariat

Brussels, 15 June 2022

WK 8681/2022 INIT

LIMITE

TELECOM

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Data Act - SI comments - Articles (doc. 6596/22)

Delegations will find in annex SI comments on "Data Act" (doc. 6596/22).

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)		We suggest that the concerns, recommendations and suggestions expressed in the EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted od 4 May 2022, with regard to the fundamental rights implications of the proposal, are taken into account as much as possible, such as the implications on the rights of access, use and share of data in relation to the existing data protection law and the lawfulness, necessity and proportionality of the obligation to make data available in case of exceptional need.
CHAPTER I GENERAL PROVISIONS		
Article 1 Subject matter and scope		

1. This Regulation lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest:		
2. This Regulation applies to:		
(a) manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services;		
(b) data holders that make data available to		

data recipients in the Union;		
(c) data recipients in the Union to whom data are made available;		
(d) public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request;		
(e) providers of data processing services offering such services to customers in the Union.		
3. Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal		

equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities. Insofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679.		
4. This Regulation shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or		This paragraph (or a new paragraph) should include also a provision that the Data Act should not affect the Union and national legal acts on protection of intellectual property rights (except

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 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		in cases referred to in Article 35 of the Data Act). Definition of data includes among others sound, visual or audio-visual recordings. Such data could be copyright protected because the definition of data contains no limitation to machine generated data. According to the recital 17 it includes data recorded intentionally by the user. "Data generated by the use of a product" (Article 1, paragraph 1) could also mean e. g. when a camera is used, audio-visual recording is made and such recording could be audio-visual work protected by copyright (or similarly, it would apply for photographs when user would use camera for taking photographs).

[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).

security, customs and tax administration and the health and safety of citizens in accordance with Union law.		
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;	'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;	From this definition (and Article 1, paragraph 1) it is not clear that the data refers only to data, which is machine generated data. According to the recital 17 it includes data recorded intentionally by the user. This means that e. g. when using a camera, audio-visual recording is made and such recording could be audio-visual work protected by copyright. Or it could mean non-copyrighted data protected by sui generis right of the maker of the database. Information

		is usually based on data.
(2) 'product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data;		
(3) 'related service' means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions;		
(4) 'virtual assistants' means software that can process demands, tasks or questions including based on audio, written input, gestures		

or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices;		
(5) 'user' means a natural or legal person that owns, rents or leases a product or receives a services;	'user' means a natural or legal person that owns, rents or leases a product or receives a services **with a legal basis**;	This definition could also cover consumers, even though it was explained (at the workshops) that the consumers were excluded. In Recital 22 it is stated that virtual assisstants play an increasing role in digitising consumer environements […]. If Data Act is meant to cover industrial data only then consumers should be excluded. If it should cover consumers as well, there should be clear line if and/or how and to what extent Data Act affects consumer protection legislation. As the definition stands at the moment, it theoretically enables a situation, when a person lends a mobile phone to another. In this situation a

		question arises - who counts as a user in this situation? The legal owner still has legal basis in legal ownership while the "new user" has legal basis as a recipient of service. **We think we should add to the definition that a user is the person who is an economic user of the product with a legal basis.**
(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;	'data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data;	We suggest additional reflection on a more clear definition of a term and all other roles related terms. Non-personal data could still be other legally protected data. We suggest to use definition from DGA.
(7) 'data recipient' means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related		

service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law;		
(8) 'enterprise' means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession;		
(9) 'public sector body' means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;	'public sector body' means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law;	We suggest t use this definition from ODD. And also definition of 'bodies governed by public law.

(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);		Very broadly defined, but it can have devastating consequences. It is not clerly specified under what conditions emergency exists? Who and by what procedure proclaims the state of emergency? How does the term relate to the institute of State of Emergency and State of War? What is allowed and what not when state of emergency is proclaimed? There is no need to define the duration of such a state? Etc.
(11) 'processing' means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;		
(12) 'data processing service' means a digital		

service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature;		
(13) 'service type' means a set of data processing services that share the same primary objective and basic data processing service model;		
(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;		
(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;		
(17) 'electronic ledger' means an electronic ledger within the meaning of Article 3, point		

(53), of Regulation (EU) No 910/2014;		
(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;		
(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		
Article 3 Obligation to make data generated by the use of products or related services accessible		
1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.		
2. Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format:		
(a) the nature and volume of the data likely		

to be generated by the use of the product or related service;		
(b) whether the data is likely to be generated continuously and in real-time;		
(c) how the user may access those data;		
(d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used;		
(e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established;		
(f) the means of communication which		

enable the user to contact the data holder quickly and communicate with that data holder efficiently;		
(g) how the user may request that the data are shared with a third-party;		
(h) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31.		
Article 4 The right of users to access and use data generated by the use of products or related services		***The user shall not use the obtained data pursuant to a request referred to in paragraph 1 to develop product or obtain information that can jeopardise public or national security.***
1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data		

generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.		
2. The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.		
3. Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade		

secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.		
4. The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate.		
5. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.		
6. The data holder shall only use any non-		The prohibition of use of data should not cover

personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.		only prohibition to derive insights about economic situation, assests and production methods of or use by the user (that could undermine commercial position of the user), it should include prohibition of use of data for the profiling of natural persons.
Article 5 Right to share data with third parties		
1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data		

holder and, where applicable, continuously and in real-time.		
2. Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of [Regulation XXX on contestable and fair markets in the digital sector (Digital Markets Act)[2]], 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);		

[2] OJ […].

(b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;		
(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).		
3. The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.		
4. The third party shall not deploy coercive		

means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.		
5. The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.		
6. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where		

relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.		
7. Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.		
8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the		

confidentiality shall be specified in the agreement between the data holder and the third party.		
9. The right referred to in paragraph 1 shall not adversely affect data protection rights of others.		
Article 6 Obligations of third parties receiving data at the request of the user		***The user shall not use the obtained data pursuant to a request referred to in paragraph 1 to develop product or obtain information that can jeopardise public or national security.***
1. A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose.		

2. The third party shall not:		
(a) coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user;		
(b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is necessary to provide the service requested by the user;		
(c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;		

(d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article […] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)];		
(e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose;		
(f) prevent the user, including through contractual commitments, from making the data it receives available to other parties.		
Article 7 Scope of business to consumer and business to business data sharing obligations		

1. The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise.		
2. Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service.		
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		
1. Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV.		
2. A data holder shall agree with a data recipient the terms for making the data available. A contractual term concerning the access to and use of the data or the liability and		

remedies for the breach or the termination of data related obligations shall not be binding if it fulfils the conditions of Article 13 or if it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.		
3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, it shall be for the data holder to demonstrate that there has been no discrimination.		
4. A data holder shall not make data		

available to a data recipient on an exclusive basis unless requested by the user under Chapter II.		
5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law.		Which "other applicable Union law or national legislation implementing Union law" is meant here (Digital Governance Act, Digital Services Act, Digital Markets Act, Artificial Intelligence Act or any other)? Any obligation under other applicable Union law or national legislation implementing Union law should be excluded from this provision (as it should be covered by that legislation itself).
6. Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU)		

2016/943.		
Article 9 Compensation for making data available		Can it be clarified in which actual case scenarios the data holder will be entitled to a payment for the transmission of data (especially under Chapter V)? Could user also be entitled to compensation?
1. Any compensation agreed between a data holder and a data recipient for making data available shall be reasonable.		
2. Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly.		

3. This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.		
4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.		
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.		This provision covers also the cross-border aspect (if dispute has been brought before dispute settlement body in another Member State)? What if there are several disputes in different Member States with data holders and data recipients from different Member States)? Can users also use this dispute settlement body?
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).		

2. A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, shall without undue delay, unless the data holder or the user instruct otherwise:		
(a) destroy the data made available by the data holder and any copies thereof;		
(b) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation,		

export or storage of infringing goods for those purposes, and destroy any infringing goods.		
3. Paragraph 2, point (b), shall not apply in either of the following cases:		
(a) use of the data has not caused significant harm to the data holder;		
(b) it would be disproportionate in light of the interests of the data holder.		
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		There should be also a similar provision regarding unfair contracutal terms unilaterally imposed on users.
1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair.		
2. A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.		
3. A contractual term is unfair for the		

purposes of this Article if its object or effect is to:		
(a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;		
(b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations;		
(c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.		

4. A contractual term is presumed unfair for the purposes of this Article if its object or effect is to:		
(a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;		
(b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;		
(c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is		

not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;		
(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		What is the relationship between this Chapter V and Article 9 of the Database Directive (in our view, the provisions of Chapter V restrict the sui generis right of database makers and this Chapter V consequently interferes with Article 9 of the Database Directive)? We understand that data collected by the sensors of a product are not considered to be protected under sui generis right of the maker of a database, but due to the definition of data and the scope of this Data Act (see Article 1), some databases protected by sui generis right could, in our understanding, fall within the scope of this Data Act. Exceptional need is never defined. It just seems

		to exist? We propose it should be defined more narrowly.
Article 14 Obligation to make data available based on exceptional need		
1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.		
2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.		
Article 15 Exceptional need to use data		
An exceptional need to use data within the		Exeptional needs should be defined narrowly.

meaning of this Chapter shall be deemed to exist in any of the following circumstances:		These conditions are set as very wide and undetermined alternatives (especially point (c)).
(a) where the data requested is necessary to respond to a public emergency;		Who determines what is public emergency? How does this provision apply if public emergency is declared in one Member State but not in other Member State(s)? The term must be defined very conservatively and restrictive with very clear procedure established by law. In existing state the chapter is huge erosion of the rule of law.
(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		Who defines when "lack of available data"

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		occurs? Which "specific tasks in the public interest" are covered and who decides which specific task in the public interest is covered by this provision? Any and all specific tasks in public interest should not be considered as exceptional need. If a special task in the public interest is explicitly provided by law, then also the obligation to provide available data should be determined in that same law. Exceptional need is not defined or at least somehow framed. We jump from public emergency to fulfilling a task in public interest, which are two totally different things and aspects. Recital 58 gives us a glimpse in very non urgent situations for such a harsh possible action.
(1) the public sector body or Union		Who determines that "existing obligation to

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		make data available" is not enough and that this provision could override the existing legislation?
(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.		This could mean overriding the existing legislation (administrative burden should be determined in existing legislation). Who would decide on this?
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		Could "fulfilling a specific task in the public interest" (from Article 15, point (c)) also be one

purposes of reporting, complying with information requests or demonstrating or verifying compliance with legal obligations.		of the obligations determined in Article 16(1)?
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		It is not specified, who declares an exceptional

Requests for data to be made available		need? Is this ment government declares exceptional need or single public sector body, e.g. one ministry?
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;		Broad definition of a term gives way for arbitrary and nondemocratic decisions. Economic stability and substantial degradation of economic assets can be many things (not to get to climate conditions, where we obviously failed). According to our way of life it is very possible they will become ordinary parts of our lives.
(c) explain the purpose of the request, the		We suggest to use similar mechanism as GDPR

intended use of the data requested, and the duration of that use;		**Data protection impact assessment.**
(d) state the legal basis for requesting the data;		Does this mean, a special law should be enacted which would define the conditions, procedures and accountability of declaring public emergency and exceptional need?
(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;		We would kindly ask for clarification, in which actual case scenarios would the data holder be entitled to a payment for the transmission of data (especially under Chapter V)? In case a public sector body would be aware that the mere publication of its request for data to be available would lead to the breach of intellectual property rights or disclosure of trade secrets, would it then in such situation still have to publish such request for data to be available?
(d) concern, insofar as possible, non-personal data;		
(e) inform the data holder of the penalties		

that shall be imposed pursuant to Article 33 by a competent authority referred to in Article 31 in the event of non-compliance with the request;		
(f) be made publicly available online without undue delay.		
3. A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024. Directive (EU) 2019/1024 shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.		Data Governance Act should also be listed here.
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		In what relationship is this provision regarding the wording "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

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.		third party" in relations to the provisions of Article 16 (e.g. verifying compliance with legal obligations or prevention, investigation, detection and prosecution of administrative offences, etc.)?
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).		
4. If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.		
5. Where compliance with the request to make data available to a public sector body or a Union institution, agency or body requires the		

disclosure of personal data, the data holder shall take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data.		
6. Where the public sector body or the Union institution, agency or body wishes to challenge a data holder's refusal to provide the data requested, or to seek modification of the request, or where the data holder wishes to challenge the request, the matter shall be brought to the competent authority referred to in Article 31.		
Article 19 Obligations of public sector bodies and Union institutions, agencies and bodies		
1. A public sector body or a Union institution, agency or body having received data		

pursuant to a request made under Article 14 shall:		
(a) not use the data in a manner incompatible with the purpose for which they were requested;		
(b) implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects;		
(c) destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data have been destroyed.		
2. Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be		

required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public sector body or the Union institution, agency or body shall take appropriate measures to preserve the confidentiality of those trade secrets.		
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		
1. A public sector body or a Union institution, agency or body shall be entitled to share data received under this Chapter with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was		

requested, or to national statistical institutes and Eurostat for the compilation of official statistics.		
2. Individuals or organisations receiving the data pursuant to paragraph 1 shall act on a not-for-profit basis or in the context of a public-interest mission recognised in Union or Member State law. They shall not include organisations upon which commercial undertakings have a decisive influence or which could result in preferential access to the results of the research.		
3. Individuals or organisations receiving the data pursuant to paragraph 1 shall comply with the provisions of Article 17(3) and Article 19.		
4. Where a public sector body or a Union institution, agency or body transmits or makes data available under paragraph 1, it shall notify		

the data holder from whom the data was received.		
Article 22 Mutual assistance and cross-border cooperation		
1. Public sector bodies and Union institutions, agencies and bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.		
2. Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested.		
3. Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the		

competent authority of that Member State as referred to in Article 31, of that intention. This requirement shall also apply to requests by Union institutions, agencies and bodies.		
4. After having been notified in accordance with paragraph 3, the relevant competent authority shall advise the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the relevant competent authority into account.		
CHAPTER VI		
SWITCHING BETWEEN DATA		

PROCESSING SERVICES		
Article 23 Removing obstacles to effective switching between providers of data processing services		
1. Providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:		
(a) terminating, after a maximum notice period of 30 calendar days, the contractual agreement of the service;		

(b) concluding new contractual agreements with a different provider of data processing services covering the same service type;		
(c) porting its data, applications and other digital assets to another provider of data processing services;		
(d) maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, in accordance with Article 26.		
2. Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the original provider.		

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 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		
Article 28 Essential requirements regarding interoperability		
1. Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services:		

(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;		
(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;		
(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;		
(d) the means to enable the interoperability		

of smart contracts within their services and activities shall be provided.		
These requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements coming from other Union or national sectoral legislation.		
2. The Commission is empowered to adopt delegated acts, in accordance with Article 38 to supplement this Regulation by further specifying the essential requirements referred to in paragraph 1.		With a goal of simplified use and enhanced transparency of data we suggest that essential requirements for interoperability should be published, properly categorized, described and available in one location for all EU stakeholders (enterprises, citizens and others) for efficient and quick overview of available data, conditions for access, (re)use and other conditions and characteristics.
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 data sharing, such as regarding rights to access and technical translation of consent or permission.		
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		
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		
1. Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of this		

Regulation. Member States may establish one or more new authorities or rely on existing authorities.		
2. Without prejudice to paragraph 1 of this Article:		
(a) the independent supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to the processing of personal data;		
(b) for specific sectoral data exchange issues related to the implementation of this Regulation,		

the competence of sectoral authorities shall be respected;		
(c) the national competent authority responsible for the application and enforcement of Chapter VI of this Regulation shall have experience in the field of data and electronic communications services.		
3. Member States shall ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of this Article are clearly defined and include:		
(a) promoting awareness among users and entities falling within scope of this Regulation of the rights and obligations under this Regulation;		
(b) handling complaints arising from alleged		

violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;		
(c) conducting investigations into matters that concern the application of this Regulation, including on the basis of information received from another competent authority or other public authority;		
(d) imposing, through administrative procedures, dissuasive financial penalties which may include periodic penalties and penalties with retroactive effect, or initiating legal proceedings for the imposition of fines;		

(e) monitoring technological developments of relevance for the making available and use of data;		
(f) cooperating with competent authorities of other Member States to ensure the consistent application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;		
(g) ensuring the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V;		
(h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI are enforced consistently with other Union legislation and self-regulation applicable to providers of data processing service;		

(i) ensuring that charges for the switching between providers of data processing services are withdrawn in accordance with Article 25.		
4. Where a Member State designates more than one competent authority, the competent authorities shall, in the exercise of the tasks and powers assigned to them under paragraph 3 of this Article, cooperate with each other, including, as appropriate, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679, to ensure the consistent application of this Regulation. In such cases, relevant Member States shall designate a coordinating competent authority.		
5. Member States shall communicate the name of the designated competent authorities		

and their respective tasks and powers and, where applicable, the name of the coordinating competent authority to the Commission. The Commission shall maintain a public register of those authorities.		
6. When carrying out their tasks and exercising their powers in accordance with this Regulation, the competent authorities shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party.		
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.		
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		
In order not to hinder the exercise of the right of users to access and use such data in accordance		This Article is amending Article 1 of the Database Directive, which determines its scope,

with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the *sui generis* right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.		or Article 7 of this Directive, which determines the sui generis right of the database producer. The Data Act restricts in Chapter V (five) the sui generis right of the maker of the database and thus affects Article 9 of the Database Directive. We would therefore kindly ask for clarification on the relationship between Chapter V of the Data Act in relation to Article 9 of the Database Directive (if a camera is used, it may collect data, which can result in copyright protected photography or audio-visual work).
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.		
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:		
(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.		
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**