Council of the European Union
General Secretariat

Brussels, 21 November 2022

WK 16035/2022 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.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Data Act Regulation DE comments on 2nd compromise text

Delegations will find in the annex the DE comments on the 2nd compromise text on Data Act Regulation.

MEMBER STATE comments on second compromise proposal on DA (document 14019/22)

Reference	Third compromise proposal	Drafting suggestion	Comment
			General Scrutiny Reservation: The proposal needs further analysis and discussion. The following remarks are preliminary and without prejudice to further changes and amendments. Further remarks at a later date reserved. Scrutiny Reservation Concerning differentiation of scopes of Data Act and Data Protection Law: A central point of criticism of the regulation proposal concerns the systematic relation to other EU and member state legislation, which in the opinion of the German government leaves many questions unanswered, including, but not limited to, the GDPR (Regulation (EU) 2016/679) and sector specific member state data protection law. As stated in the Data Act Proposal the Regulation is without prejudice to the GDPR. However, in spite of this declaration, overlaps, contradictions, unclear definitions and inconsistencies regarding wording or regulatory gaps concerning fundamental issues remain. In addition, it should be clarified how the data-relevant European laws apply in a coherent manner. The need for

Reference	Third compromise proposal	Drafting suggestion	Comment
			clarification in the submitted draft is also reflected by the fact that, due to redundancies in normative texts, it cannot yet be clearly concluded whether individual provisions of the Data Act or the GDPR apply. DEU advocated for a more precise differentiation of the scopes between Data Act and data protection law. It must be made clear that the processing of data sets containing personal data is subject to the applicable data protection legal framework, in particular the GDPR and the national regulations based on it. Concerning: differentiation between B2C and B2B-rules in the Data Act: Stakeholders have consistently called for greater differentiation in the legal design of data access and data use rules in Chapter II. While stakeholders in the B2B sector - within the framework of the applicable data protection and competition law - advocate for more leeway under contract law. Stakeholders in the customer sector, especially consumers, demand specific consideration of consumer interests and a stronger legal position vis-à-vis other players in the data economy.

Reference	Third compromise proposal	Drafting suggestion	Comment
			The German government's aim is to reconcile the objectives of the Data Act with the fundamental rights to the protection of personal data, to scientific freedom and to entrepreneurial freedom. The Data Act is intended to deliver a positive balance of innovation and investment, and to take a coherent approach that avoids unnecessary bureaucracy and transaction costs. In addition to improving access to data, the German government also aims to strengthen the data portability of this data so that users retain control over their data and make independent decisions with regard to corresponding available options, as well as to give other economic players the opportunity to use the data for purposes that are in the interest of the users. The aim is to also ensure a fair data-based economy for consumers and keeping in focus that the data economy must also benefit the public interest. As a contribution to achieving these goals, the German government is considering creating incentives in the B2C sector to promote data use and prohibit unfair business practices by Union law, e.g. data access and reuse by

Reference	Third compromise proposal	Drafting suggestion	Comment
			third parties. These unfair business practices could be inter alia: Data use for AI systems, which will be prohibited under the AI Regulation (AI Act), data use for the purpose of profiling, which is not strictly necessary to provide a service, and de-anonymization of data. Concerning access of research organisations and researchers to privately held data (e.g. companies): In addition to the B2G access rules in Art. 15 of the DA Draft, the German government is considering proposing accesses for public research institutions to private sector data in the substantial public interest in order to foster the innovation potential of data in science. Such Union-wide harmonized data access rules for research purposes must be concise, proportionate and designed in accordance with data protection rules, in particular taking into account a close proximity to a research organization, independence from commercial interests, the preservation of trade secrets and the restriction to research projects of substantial public interest and with cross-border relevance. Existing and future sector-specific regulations,

Reference	Third compromise proposal	Drafting suggestion	Comment
			concerning inter alia health data, will be respected and their prevalence will not be undermined. Consequently, these prevalent access regulations must block the application of the Data Act.
Recital 5	(5) This Regulation ensures that users of a product or related service in the Union can access, in a timely manner, the data generated by the use of that product or related service and that those users can use the data, including by sharing them with third parties of their choice. It imposes the obligation on the data holder to make data available to users and third parties nominated by the users in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and in a transparent manner. Private law rules are key in the overall framework of data sharing. Therefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances that hinder fair data access and use for micro, small or medium-sized enterprises within the meaning of Recommendation 2003/361/EC. This Regulation also ensures that data holders make available to public sector bodies of the Member States and to Union institutions, agencies or bodies, where there is an		We request clarification as to whether the Data Act contains additional legal bases for the processing of personal data against the background of Recital 5 and to answer the question whether the access (Art. 4) and disclosure (Art. 5) rules regarding personal data are to be regarded as a legal basis within the meaning of the GDPR.

Reference	Third compromise proposal	Drafting suggestion	Comment
	exceptional need, the data that are necessary for the performance of tasks carried out in the public interest. In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union. This Regulation should not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service. Instead, it takes as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services.		
Recital 14		(14) Physical products that obtain, generate or collect, by means of their components **or operating system**, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) ~~should be~~ **are** covered by this Regulation.	"are covered" instead of "should be covered": this ought to be a statement of fact.
Recital 15	In contrast, certain products that are primarily designed to display or play content, **such as textual or audiovisual, often covered by intellectual property rights,** or to record and	In contrast, certain products that are primarily designed to display or play content, **such as textual or audiovisual, often covered by intellectual property rights,** or to record and	The reasoning for including smart watches in scope of Data Act is arbitrary ("have a strong element of collection of

Reference	Third compromise proposal	Drafting suggestion	Comment
	transmit **such** content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, ~~personal computers, servers, tablets and smart phones,~~ **smart televisions and speakers,** cameras, webcams, sound recording systems and text scanners. **Additionally, products primarily designed to process and store data, such as personal computers, servers, tablets and smart phones, should not fall in scope of this Regulation.** ~~They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.~~ **On the other hand, smart watches have a strong element of collection of data on human body indicators or movements and should thus be considered covered by this Regulation as far as they qualify as ~~the definition of~~ "product" in particular due to the ability to communicate data via a publicly available electronic communication service. Given the share of investment in providing data-related functions in relation to other functions of these categories of products, the oligation to allow access or the sharing of data would be disproportionate in the light of the objective of this Regulation.**	transmit **such** content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, ~~personal computers, servers, tablets and smart phones,~~ **smart televisions and speakers,** cameras, webcams, sound recording systems and text scanners. **Additionally, products primarily designed to process and store data, such as personal computers, servers, tablets and smart phones, should not fall in scope of this Regulation.** ~~They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.~~ **On the other hand, smart watches have a strong element of collection of data on human body indicators or movements and should thus be considered covered by this Regulation as far as they qualify as ~~the definition of~~ "product" in particular due to the ability to communicate data via a publicly available electronic communication service. ~~Given the share of investment in providing data-related functions in relation to other functions of these categories of products, the oligation to allow access or the sharing of data would be disproportionate in the light of the objective of this Regulation.~~**	data"). The differentiation should be along those lines, whether they are primarily designed to play content (like a Smart TV, which they are not) or whether they are connected to the internet and collect and process data for the service they provide (like an IoT-device, which they are). Furthermore, are cameras installed in a car covered by the scope, but cameras connected via an interface are not? Similar questions arise when a smart device is controlled via an app installed on a smart phone or tablet. Does the data generated on a smart phone or tablet not fall under the Data Act?

Reference	Third compromise proposal	Drafting suggestion	Comment
Recital 29	**They could play an instrumental role in aggregating access to data from a large number of individual users so that big data analyses or machine learning can be facilitated, as long as such users remain in full control on whether to contribute their data to such aggregation and the commercial terms under which their data will be used.**	**They could play an instrumental role in aggregating access to data from a large number of individual users so that big data analyses or machine learning can be facilitated,** as long as such users **retain** full control o~~n~~**fn** whether to contribute their data to such aggregation and **of** the commercial terms under which their data will be used.	We suggest making the following changes in order to provide more clarity on the meaning of the text.
Recital 39	(39) Based on the principle of contractual freedom, the parties should remain free to negotiate the precise conditions for making data available in their contracts, within the framework of the general access rules for making data available. **Such terms could include technical and organisational issues, including in relation to data security.**		We ask to clarify whether this addition indicates that the level of security of processing required by e.g. GDPR or other relevant regulation is seen as negotiable
Recital 42	In order to incentivise the continued investment in generating valuable data, including investments in relevant technical tools, **while at the same time avoiding excessive burden for access and use of data which make data sharing no longer commercially viable,** this Regulation contains the principle that the data holder may request reasonable compensation when legally obliged to make data available to the data recipient.	In order to incentivise the continued investment in generating valuable data, including investments in relevant technical tools, **while at the same time avoiding excessive burden for access and use of data which make data sharing no longer commercially viable,** this Regulation contains the principle that the data holder may request reasonable compensation when legally obliged to make data available to the data recipient. **The costs associated with anonymising pseudonymising data which is made available directly to data recipients**	

Reference	Third compromise proposal	Drafting suggestion	Comment
		may be included in the compensation agreed.	
Recital 50a	In the case of abusive practices such as misleading the data holder with inaccurate information …	In the case of abusive practices **on the part of the data recipient,** such as misleading the data holder	We suggest making the following changes in order to provide more clarity on the meaning of the text.
Recital 74	Data processing service providers should be required to offer all assistance and support that is required to make the switching process **to a service of a different data processing service provider** successful**,** and effective. **and secure including in cooperation with the data processing service provider of the destination service. Data processing service providers should also be required to remove existing obstacles and not impose new for customers wishing to switch, also, to an on-premise system. Obstacles relate to, inter alia, hurdles of commercial, technical, contractual and organisational nature. Throughout the switching process, a high level of security should be maintained. This means that the data processing service provider of the original data processing service should extend the level of security to which it committed for the service to all technical modalities deployed in the related switching process (such as network connections or physical devices). This Regulation does not require** without requiring those data processing service providers to develop new categories of services within or on the basis of the IT-		We ask the Commission whether it can be ensured that it becomes apparent in which cases the obstacles are related to the original provider.

Reference	Third compromise proposal	Drafting suggestion	Comment
	infrastructure of different data processing service providers to guarantee functional equivalence in an environment other than their own systems. Nevertheless, service providers are required to offer all assistance and support that is required to make the switching process effective. Existing rights relating to the termination of contracts, including those introduced by Regulation (EU) 2016/679 and Directive (EU) 2019/770 of the European Parliament and of the Council[13] should not be affected.		
Recital 79	[…] Operators within the data spaces, which are entities facilitating or engaging in data sharing within the common European data spaces, including data holders, should comply with these requirements in as far as elements under their control are concerned. […]		DEU asks whether the clarification of data holders falling within the scope of "operators within data spaces" should be included in the definition of Art. 2 (15a) or in the essential requirements regarding interoperability of Art. 28.
Art. 1 (4)	4. **This Regulation does not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities.** 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	4. This Regulation 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	Example for wording based on NIS 2 Directive.

Reference	Third compromise proposal	Drafting suggestion	Comment
	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 security, customs and tax administration and the health and safety of citizens in accordance with Union law~~.~~ **or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.**	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.	

[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).

Reference	Third compromise proposal	Drafting suggestion	Comment
		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.	
Art. 3 (1)	Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use **that are readily available to the data holder** are, by default **and free of charge**, easily, securely and, where relevant and appropriate, directly accessible to the user**., in a structured, commonly used and machine readable format.**		Regarding the fundamental change from "accessible" to "readily available" data in Art. 3, the Council Presidency is asked to explain the effects.
Art. 3 (2c)	how the user may access those data **including in view of the data holder's data storage and retention policy;**		We ask the COM why if it is necessary to specify the data holder's storage and retention policies? Further, could storage and retention be used as a loophole

Reference	Third compromise proposal	Drafting suggestion	Comment
			through which data-sharing can be avoided (e.g. company's storage policy is only one week)?
Art. 4 (1a)	Any agreement between the data holder and the user shall not be binding when it narrows the access rights pursuant to paragraph 1.		We continue to raise the fundamental question of whether a clearer distinction between B2B and B2C is necessary in the provisions in the Data Act. We explore whether additional provisions in the Data Act (particularly protections in the B2C area) are needed. In particular, in the B2C area, we examine how the goal of the Data Act (to fairly allocate the value of data among stakeholders in the data economy and to promote data access and use) can best be achieved while taking into account the fundamental rights of personal data protection, scientific freedom, and freedom of economic activity.
Art. 4 (5)	Where the user is not a **the** data subject **whose personal data is requested,** 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 **and Article 5(3) of**	~~Where the user is not a **the** data subject **whose personal data is requested,** 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 **and Article 5(3) of***	Scrutiny reservation: This question is answered by applicable data protection law and should not be addressed by the Data Act.

Reference	Third compromise proposal	Drafting suggestion	Comment
	Regulation Directive (EU) 2002/58 are fulfilled.	~~**Regulation Directive (EU) 2002/58** are fulfilled.~~ Data holders should make best efforts to ensure that personal data is only accessed by users the data refers to and that there is a valid legal basis for the user to receive personal data of data subjects other than himself.	
Art. 5 (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 that are accessible readily available to the data holder to a third party, as well as the relevant metadata, without undue delay, free of charge to the user, of the same quality as is available to the data holder, easily, securely, in a structured, commonly used and machine-readable format and, where applicable, continuously and in real-time. The making available of the data by the data holder to the third party This shall be done in accordance with the conditions and compensation rules set in Articles 8 and 9.		Art. 5(1) now explicitly refers to the compensation provisions of Art. 8 and 9. Can this lead to a situation where the compensation arrangements possible between data holders and third parties will result in costs being passed on to consumers?
Art. 6 (2) (a)	The third party shall not: (a) coerce, deceive or manipulate ~~in any way and at any time~~ the user **or the data subject where the user is not a data subject**, ~~in any way~~, by subverting or impairing the		We are examining ways to prevent certain commercial practices, most importantly those that are incompatible with fundamental right to data protection, and ask the Presidency, other

Reference	Third compromise proposal	Drafting suggestion	Comment
	autonomy, decision-making or choices of the user **or the data subject**, including by means of a digital interface with the user **or the data subject**;		Member States and the Commission for their opinion on this matter."
Art. 6 (2aa)		aa) use anonymised data for the processing of data in such a manner that it can be attributed to a specific data subject (de-anonymisation);	
Art. 11			We believe that in cases of third parties' unauthorised use of data, penalties or compensation requirements should be specified.
Art. 11 (2a)	Where the data recipient has acted in violation of Article 6(2)(a) and 6(2)(b), users shall have the same rights as data holders under paragraph 2. Paragraph 3 shall apply mutatis mutandis.		Scrutiny Reservation: Given the scope ("user") and the consequences ("end the production, offering, placing on the market or use of goods, etc.") of the proposal the Commission is asked to clarify whether this provision is necessary and proportionate.
Art. 11 (3)		(c) the data holder and the user of the product and related service have received payment by the data recipient for any damages incurred.	Proposal in the interest of proportionality
Art. 13	Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise		The scope of Article 13 should not be limited to terms used in contracts with SMEs. According to recital 51, the use of terms in contracts with large companies also entails a risk of the user leveraging its stronger bargaining position to exploit the weaker position of the other party.

Reference	Third compromise proposal	Drafting suggestion	Comment
			When a contract is concluded between two larger companies and one of the parties holds sufficient market power to impose contract terms on the other, Germany sees no reason to deny one company the protection of fairness checks. This also avoids the difficulties of defining companies in terms of their size at the time of conclusion of the contract, as the criteria set out in Recommendation 2003/261/EC cannot be ascertained with legal certainty for all companies at the time of conclusion of the contract. It is especially difficult to reliably ascertain these criteria for the contracting party that unilaterally imposed the terms if a company's status has frequently shifted between SME and large company in the past.
Art. 13 (1)	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**, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation**	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 **another enterprise** ~~a micro, small or medium-sized enterprise 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~~	Insertion of "another enterprise" and deletion from "a micro...": Expansion of the scope of application to include all contracts and not just those with SMEs. **Substantive scope of application** According to information provided by the Commission, Article 13 should apply to all contractual agreements on data, even where there is no right of access

Reference	Third compromise proposal	Drafting suggestion	Comment
	2003/361/EC which do not qualify as a micro, small or medium enterprise, shall not be binding on the latter enterprise if it is unfair.	~~defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro, small or medium enterprise,~~ shall not be binding on the latter enterprise if it is unfair.	pursuant to Article 5 of the Data Act. According to the definitions in Article 1 (1 to 3) this includes both personal and non-personal data. Why is Article 13 not limited to the cases specified in Article 8? The cases listed in Article 8 (right pursuant to Article 5 of the Data Act or rights arising from other legal acts) comprise material standards that could provide a benchmark in the matter of fairness, and could thus serve as a model in the application of fairness checks in the courts of the individual Member States with respect to contractual agreements that go beyond statutory requirements. However, a uniform benchmark of this sort under European Union law is lacking for those contractual agreements that were concluded independently of existing access rights. Are uniform fairness checks on the basis of Article 13 even possible for “voluntary agreements” of this kind? Would such a broad provision still fall under the legal basis of Article 114 TFEU? Germany kindly requests an assessment by the Council’s Legal Service of the extent to which the provisions on unfair contract terms can be based on Article

Reference	Third compromise proposal	Drafting suggestion	Comment
			114 TFEU if they are to be applicable to all contracts governing data use. On the scope of application, here: "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": To what extent is Article 13 conclusive, with the result that national provisions governing fairness checks are ruled out by the Data Act? Would this limitation of scope mean that a contract containing provisions such as those specified and other contractual provisions might have to be subjected to two separate fairness checks? I.e., according to Article 13 for data-related terms, and according to the fairness benchmark provided for by national law with regard to other terms (e.g. delayed monetary compensation, offsetting, etc.)? What is the legal status of mixed contracts? How are standard contract terms agreed both for data use and for other contractual services to be evaluated? Can they be deemed ineffective in their totality if they are in violation either of the Act or of national law, or must they be deemed effective

Reference	Third compromise proposal	Drafting suggestion	Comment
			with regard to data use if they are not in violation of Article 13?
Art. 13 (2)	A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.	2. A contractual term is unfair **if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment to the party upon whom the contractual term has been unilaterally imposed.** ~~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~~.	We consider Paragraph 2 as proposed not a suitable benchmark for fairness checks as it raises too many questions and is not conducive to the desired harmonisation of laws. Which sphere of commercial practice is intended (regional, national or European commercial practice)? Can a European commercial practice emerge from different contract law systems? What happens until a commercial practice has emerged for new contracts? Who shapes commercial practice (the companies that succeed in imposing their contract terms on the market?) How can the relevant commercial practice be ascertained by the courts? Under what conditions is a commercial practice to be considered "good"? Why not consider every deviation from good commercial practice to be unfair, as opposed to merely gross deviations? What constitutes a gross deviation? Recital 2 points to the current existence of "abuse of contractual imbalances with regards to data access and use". This suggests that whereas commercial practice exists, it is not necessarily good

Reference	Third compromise proposal	Drafting suggestion	Comment
			commercial practice. If there is no good commercial practice, where should a court seek the general benchmark by which to evaluate contract terms? Accordingly, Germany believes that it makes more sense to specify an assessment benchmark that carries greater legal weight. Such a standard has been in place for years in Directive 93/13/EEC. This standard permits verification against existing contract law. Given that the contract law applicable to b2b contracts is different from that applicable to b2c contracts, the standard provides a separate benchmark for each case. What is the relationship between the definition of "unfairness" in Article 13(2) and the FRAND requirement in Article 8(1)?
Art. 13(3)	A contractual term is unfair for the purposes of this Article paragraph 2, in particular if its object or effect is to:	3. In particular, a contractual term is unfair for the purposes of ~~this Article~~ **paragraph 2** if its object or effect is to:	Germany's view is that all unfairness conditions should be specified in a "black list". "Grey lists" create considerable legal uncertainty for both contracting parties, as at the time of conclusion of the contract they are unable to predict with certainty whether a term included in a "grey list" will be deemed ineffective or, in light of the particular

Reference	Third compromise proposal	Drafting suggestion	Comment
			circumstances of each specific case, effective. Germany is therefore in favour of including only a "black list" in the catalogue, but rewording the terms in such a way as to make them fit for purpose and to allow sufficient leeway for evaluation in light of the facts of the case at hand. This also allows individual unfairness conditions to be listed together. The insertion of "especially" is suggested in order to make it clear that this is simply a specific manifestation of the general clause in paragraph 2.
Art. 13 (3a)	exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;	(a) **inappropriately** exclude or limit the liability of the party that unilaterally imposed the term ~~for intentional acts or gross negligence~~ **or extends the liability of the enterprise upon whom the term has been imposed**	A more general wording is needed here in order to better account for the nature of the breach and the resulting damages within the unfairness condition. Otherwise, verifications on the basis of this unfairness condition and the general clause in paragraph 2 will frequently yield different results. Moreover, the unfairness condition should be expanded: as it stands, only the exclusion of liability of the party that unilaterally imposed the terms is addressed. It should also be stipulated that the party that unilaterally imposed the terms cannot also be able to

Reference	Third compromise proposal	Drafting suggestion	Comment
			unreasonably extend the liability of the other party.
Art. 13 (3b)	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;	(~~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~~;	Unnecessary if paragraph 4 (a) of the Commission's proposal is included in the black list (see letter c - new).
Art. 13 (3c)	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.	~~(c)~~ (b) 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.	Editorial amendment to the numbering.
Art. 13 (4)	A contractual term is presumed unfair for the purposes of this Article **paragraph 2** if its object or effect is to:	~~4. A contractual term is presumed unfair for the purposes of this Article **paragraph 2** if its object or effect is to:~~	See comment on paragraph 3. There should only be a black list.
Art. 13 (4a)	inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;	~~(a)~~ **(c)** inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;	Editorial amendment to the numbering.
Art. 13 (4b)	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;	~~**(b)**~~**(d)** 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;	Such a term should be ineffective if it is in any way detrimental to the legitimate interests of the party whose data is to be made available.
Art. 13 (4c)	(prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during	~~(c)~~ **(e)** prevent the party upon whom the term has been unilaterally imposed from using the	For Germany it is unclear what is meant by "proportionate" here. In Germany's

Reference	Third compromise proposal	Drafting suggestion	Comment
	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;	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;	view, the question is whether the use and value of the data are to be weighed against each other (in which case "proportionate"), or whether a wider assessment of the overall circumstances is to be undertaken (in which case "reasonable" may be preferable).
Art. 13 (4d)	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;	~~(d)~~ **(f)** 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;	Editorial amendment to the numbering.
Art. 13 (4e)	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.	~~(e)~~ **(g)** 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.	Editorial amendment to the numbering.
Art. 13 (5)	A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied **drafted in advance** 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 **drafted in advance** a **the** contractual	~~5~~ 4. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied **drafted in advance** 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 **drafted in advance** a **the** contractual	Editorial amendment to the numbering.

Reference	Third compromise proposal	Drafting suggestion	Comment
	term bears the burden of proving that that term has not been unilaterally imposed.	term bears the burden of proving that that term has not been unilaterally imposed.	
Art. 13 (6)	Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding.	~~6~~ **5.** Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding. **The remaining terms shall not be binding, if upholding the remaining terms would be an unreasonable hardship for one party.**	Germany asks whether the proposed wording is appropriate if, regardless of the applicable substantive law, the contract should always be upheld in such cases. If crucial terms of the contract become ineffective, it must be asked to what extent upholding the contract constitutes an unreasonable hardship for one or both parties. Germany therefore proposes a corresponding addition. The following question must also be asked: What conditions/legal situation apply if a contract term is declared ineffective? In Germany's view, the resulting legal situation is determined by the relevant applicable law. This could also be clarified.
Art. 13 (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 **nor to the adequacy of the price, as against the data supplied in exchange**.	~~7.~~ **6.** This Article does not apply to contractual terms defining the main subject matter of contract or to contractual terms determining the price to be paid **nor to the adequacy of the price, as against the data supplied in exchange**.	Editorial amendment to the numbering.
Art. 13 (8)	The parties to a contract covered by paragraph 1 may not exclude the application	~~8.~~ **7.** The parties to a contract covered by paragraph 1 may not exclude the application	Editorial amendment to the numbering.

Reference	Third compromise proposal	Drafting suggestion	Comment
	of this Article, derogate from it, or vary its effects.	of this Article, derogate from it, or vary its effects.	
Chapter V			Scrutiny Reservation: The German government aims to significantly improve the availability and use of data by the public sector. It welcomes the fact that the COM draft contains proposals in Chapter V to help achieve this common goal. A harmonized legal framework throughout the Union is fundamentally in the interests of the economy. The German government therefore supports proposals that provide the right to access data in the event of public emergencies. However, the Commission's proposals could benefit from being made more specific, both because of their breadth of scope and vagueness with regard to the proposed procedural arrangements. It should be examined whether, without harmonizing the underlying "statutory tasks" in the Data Act, sovereign access to private data should instead be regulated in specific laws. Particularly in question is the last group of cases mentioned in Article 15(c)(1), in which the "adoption of new legislative

Reference	Third compromise proposal	Drafting suggestion	Comment
			measures [...] cannot ensure the timely availability of the data." The German government asks that the provision in Article 15(c) of the DA Draft be examined and, if necessary, be made more specific in order to strike an appropriate balance between the interests of the public sector, the economy, and citizens, as well as to ensure the nature of the provision as an exception."
Article 19 (2)	In such a case, the public sector body or the Union institution, agency or Commission, the European Central Bank or Union body shall take, prior to the disclosure, appropriate measures, such as technical and organisational measures, to preserve the confidentiality of those trade secrets.	In such a case, the public sector body or the Union institution, agency or Commission, the European Central Bank or Union body shall take, prior to the disclosure, appropriate measures, such as technical and organisational measures, to preserve the confidentiality of those trade secrets, **in particular with respect to individuals or organisations receiving the data under the provisions of Article 21. Where such measures do not suffice, the data holder and the user shall agree on additional measures to preserve the confidentiality of the shared data, in particular in relation to third parties.**	Same provision for third parties should apply for third parties that receive data via a public sector body as to third parties that receive data directly via data holder. Therefore, Article 19 (2) should reflect the same provisions as Article 4(3).
Art.23	Removing obstacles to effective switching between providers of data processing services		Any regulation on the switch of contracts should be aligned with DORA.
Art 23 (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		We understand the provisions under Chapter VI as covering customers of a data processing service. These customers

Reference	Third compromise proposal	Drafting suggestion	Comment
	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**s** shall remove **not pose** commercial, technical, contractual and organisational obstacles, which inhibit customers from:		include both private individuals and enterprises, and as such would cover solo-self-employed platform workers
Art. 23 (1a)	terminating, after a **the** maximum notice period of 30 calendar days **specified in the contract in accordance with Article 24**, the contractual agreement of the service;		Are individual contractual agreements between providers and customers that provide for other transition periods possible, especially in the case of the implementation of complex projects? If not, how can the implementation costs of large projects be calculated and covered in a way that can be planned? We welcome the reference made in Article 23 (1), letter a to extend the contractual notice period to two months, but ask whether, depending on the business model, any change of data processing service can be made within the time.
Art. 23 (1b)	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.
Art. 23 (1d)	**in accordance with paragraph 2 Article 23a,** maintaining functional equivalence of the service in the IT-environment of the different		Are providers and customers able to make individual contractual arrangements that provide for different

Reference	Third compromise proposal	Drafting suggestion	Comment
	provider or providers of data processing services covering the same service type, in accordance with Article 26.		transition periods, especially in the case of the implementation of complex projects? If not, how should the implementation costs of large projects be calculated and covered in a plannable manner?
Art.24	Contractual terms concerning switching between providers of data processing services		Switching between cloud providers requires the cooperation of both the exporting and importing data processor. The Data Act places the obligations on the exporting provider, who is responsible for the switch and migration process, and who is expected to maintain continuity of services and functionality under the same conditions, but at the same time has no interest in the switch. Therefore, we ask: How does KOM intend to address this imbalance? Furthermore, has consideration been given to the fact that the regulations could have the undesirable side effect that the requirements may only be met by dominant companies (and gatekeepers)?
Art.24(1a 3)	**ensure that a high level of security is maintained throughout the porting process, notably the security of the data during their transfer and the continued security of the**		We welcome the inclusion of the additional safeguard against possible data loss during the porting. Since the transfer of data also involves the data

Reference	Third compromise proposal	Drafting suggestion	Comment
	data during the retention period specified in paragraph 1 point (c) of this article.;		processing service provider of the target service, the obligation to ensure data security should not lie solely on the side of the outgoing data processing service provider.
Art.24(1a 3 ba)	**an exhaustive specification of categories of metadata specific to the internal functioning of provider's service that will be exempted from the exportable data under point (b), where a risk of breach of business secrets of the provider exists. These exemptions shall however never impede or delay the porting process as foreseen in Article 23;**	**(ba) an exhaustive specification of categories of metadata specific to the internal functioning of provider's service that will be exempted from the exportable data under point (b), where a risk of breach of ~~business~~ trade secrets of the provider exists. These exemptions shall however never impede or delay the porting process as foreseen in Article 23;**	We suggest a consistent use of the term "trade secret" (instead of "business secret").
Art. 25	Gradual withdrawal of switching charges		Does the withdrawal of switching charges mean that specific services from third-party providers to support migration processes may no longer be offered in the future? - Switching between cloud providers requires the cooperation of both the exporting and the importing data processing service. The Data Act places the obligations on the exporting provider, who is responsible for the switch and the migration process and who is supposed to maintain continuity of services and functionalities under the same conditions, but at the same time

Reference	Third compromise proposal	Drafting suggestion	Comment
			has no interest in the switch. How does COM intend to address this imbalance? Furthermore, has it been considered that the regulations could have the undesirable side effect that the requirements may only be met by market-dominant companies (and gatekeepers)?
Art. 25 (1)	From [date X+3yrs] onwards, providers of data processing services shall not impose any charges on the customer for the switching process.		Who does the COM expect to bear the "costs" of switching in the future? Did the COM consider that providers may pass on the costs to all customers via general pricing, including exceptional costs in large B2B projects?
Art 28(1)	Operators of **within** data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services **as well as of the common European data spaces, which are purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives**:		What distinguishes an "operator within data spaces" from a "data sharing service" as defined by the DGA and what distinguishes it from a "controller" as defined by the GDPR? Operators of data spaces - insofar as they hold personal data - are likely to be responsible within the meaning of the GDPR. In terms of reducing bureaucratic costs, aligning the information requirements of Article 28 (1) with the information and documentation requirements of the GDPR (Articles 13, 14 and 30) would be desirable.

Reference	Third compromise proposal	Drafting suggestion	Comment
Art. 30	Essential requirements regarding smart contracts for data sharing		Scrutiny Reservation: To what extent does COM see a specific need for regulation of smart contracts, that is not already covered by the existing standards for software and algorithms, like EN ISO/IEC 17065 and EN ISO/IEC 17029, which could be referenced in this law? Or should smart contracts be regulated in another horizontal legal act? Also, are smart contracts necessary to reach the goals set out by Article 30? Lastly, clarification is needed on whether the scope of the definition of smart contracts should contain both distributed and central ledger options.
Art. 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, [**For the purposes of the exercise of the rights provided for in Articles 4 and 5 of this Regulation**, the sui generis right provided for in Article 7 of Directive 96/9/EC does **shall** not apply to databases containing data **when data is** obtained from or	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 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~~	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 databases containing raw data generated by IoT-Devices. However,

Reference	Third compromise proposal	Drafting suggestion	Comment
	generated by a product or related service.] OR **[T**he sui generis right provided for in Article 7 of Directive 96/9/EC **does shall** not apply to databases containing data **when data is** obtained from or generated by the use of a product or a related service.]	~~product or a related service. OR [The sui generis right provided for in Article 7 of Directive 96/9/EC does shall not apply to databases containing data when data is obtained from or generated by the use of a product or a related service.]~~	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.
Art. 31			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.
Art. 40(1)	The specific obligations for the making available of data between businesses,		It needs to be examined in more detail whether and to what extent (sector-)

Reference	Third compromise proposal	Drafting suggestion	Comment
	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 **date of entry into force of this Regulation**], and delegated or implementing acts based thereupon, shall remain unaffected.		specific and complementary regulations on data access may be possible under Member State legislation.

Kindly indicate the Member State you are representing in the Title and when renaming the document. For specifying the relevant provision, please indicate the relevant Article or Recital in 1st column and copy the relevant sentence or sentences as they are in the current version of the text in 2nd column. For drafting suggestions, please copy the relevant sentence or sentences from a given paragraph or point into the 3rd 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 providing an explanation and reasoning behind your proposal, please take use of 4th column.