Council of the European Union
General Secretariat

Brussels, 18 November 2022

WK 15990/2022 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 FI comments on 2nd compromise text

Delegations will find in the annex the FI 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 remarks: In general, we think that topics to be still jointly discussed are - Prevention of misuses of the data requests /and of the use rights - Role of the APIs - Automatisation (of contracts) - Implementation and - The role of authorities Scrutiny reservation to the text, as it has not been subject to Parliamentary approval nationally. The text by us in red means that the comment is crucially important for us (mainly due to constitutional constraints)
SCOPE and DEFINITIONS			
Article 2		'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, and under Chapter II or III, it means raw data excluding	Justification for this suggestion: to add clarity and to mirror Recital 14a. We think that the GDPR could be taken as an inspiration here (what the controller has collected). See also the

Reference	Third compromise proposal	Drafting suggestion	Comment
		aggregated, derived, inferred or further processed data	opinion by the EDPS. However, we can be flexible on this.
Article 1(2)	(c) data recipients, irrespective of their place of establishment, in the Union to whom data are made available;	(c) data recipients, ~~irrespective of their place of establishment,~~ in the Union to whom data are made available;	The data holders should be able to conduct necessary technical measures to ensure that the data access should take place only in the EU; so that there is no obligation to transfer data outside the EU/EEA. Would it be possible to mandate data holders to use technical means for instance to limit the access to application programming interphases (APIs) outside from the EU ? e.g. in the related recitals. Please see also below.
Article 1		New para 5: Unless otherwise provided by Union law or by national legislation implementing Union law, an obligation to make data available to a user or third party shall not oblige granting access or assisting transfer of data directly or indirectly, to any natural	Right to access data should be limited to EU-based access and transfers of data for third parties. Also, in a situation where the user or third party is likely to share the data to their non-EU based affiliate, the data holder and manufacturer should

Reference	Third compromise proposal	Drafting suggestion	Comment
		or legal person, entity or body outside the Union.	have the right to prevent the transfer of data from the EU also with technical means. Please see also below, art. 4(2)
Article 4(2)		The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user in the Union pursuant to paragraph 1. - -	Aim: Redefining the applicability to EU-based users. In a situation where the user or third party is likely to transfer the data to their non-EU based affiliate, the data holder - and manufacturer should have the right to prevent the transfer of data from the EU.
Article 4		New para 7: The data holder shall not be required to make data available where it has a reasonable belief that such data will be made available to users or third parties outside the Union. The data holder and the user can agree measures to prevent the data from being shared outside the Union, in particular in relation to third parties.	

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 1(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 is without prejudice to 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.	We underscore clarity and consistency between the Data Act and other EU law. There should be no room for ambiguity as to which rule(s) to follow. The issue here also relates to recital 31.
Article 2	(2) 'product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates	(2) 'product' means a tangible, movable item, including where incorporated in an immovable	The notion 'that is able to communicate data directly or indirectly via a publicly available electronic communications

Reference	Third compromise proposal	Drafting suggestion	Comment
	or collects, data concerning its use or environment, and that is able to communicate data directly or indirectly via a publicly available electronic communications service and whose primary function is not neither the storing and processing of data nor is it primarily designed to display or play content, or to record and transmit content;	item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data directly or indirectly via a publicly available electronic communications service [as defined in the European electronic communications code 1972/2018] and whose primary function is not neither the storing and processing of data nor is it primarily designed to display or play content, or to record and transmit content;	service' would necessitate for a reference to the 1972/2018 European electronic communications code, EEECC. It would seem appropriate to further precise the definition of publicly available communications services in a recital – e.g. in rec. 14, where 'publicly available communications service' is used.
Chapter V			The rights of public sector bodies to receive data under Chapter V under exceptional need seem unclear when it comes to the data under the ePrivacy directive 2002/58/EC. Based on the proposal art. 1(3) 'This regulation is without prejudice to […] Directives 2002/58/EC […]'. Also, in rec. 7: 'This Regulation complements and is without prejudice to

Reference	Third compromise proposal	Drafting suggestion	Comment
			Union law on data protection and privacy, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications.' However, this priority is not taken into account in the art. 14 of the compromise proposal. Art. 14(1) reads 'Upon request, a data holder shall make data, which could include relevant metadata, available to a public sector body or to the Commission, the European Central Bank or Union Bodies demonstrating an exceptional need to use the data requested in order to carry out their statutory duties in the

Reference	Third compromise proposal	Drafting suggestion	Comment
			public interest.' What is more, no other article in Chapter V of the proposal address the issue of so called traffic data (see. Art. 5(3) of the ePrivacy directive) which, however, are being referred to in recitals 7 and 32 of the proposal. The article 14 would seem to cover if need be any kind of data. This does not, however, take into account traffic data. When it would seem that the ePrivacy directive would have priority over the Data act as noted above, it would seem that the authorities (public sector bodies) would not have a right under Chapter V here to receive from data holders data protected under the ePrivacy directive, (such as those gathered under its art. 5(3)). However, in case the authorities (public sector

Reference	Third compromise proposal	Drafting suggestion	Comment
			bodies) would have such a right to receive such data, then the last sentence in the recital 7. ('No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications.') would be untrue. Thus, the question is (again) what data is in scope here under Chapter V, as under the ePrivacy directive such data would not cover location data of terminal equipment) nor other data from such device.
National legislation on public documents			

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 19		3. Obligations in this Article are without prejudice to Member State law on access to and retention of public documents.	National access to public documents regimes in Chp V /art. 19 (same as data governance act); How official documents are processed, stored, archived, and erased and how the public can have access to them (based on national law) should still be allowed. Access to documents and Art. 19(1)(a) and (c) : We need to take into account the conditions set out in our constitution and related to the openness of documents. This is about transparency in governance in Finland, and it is fundamentally important. Therefore, here, an important question for us is, whether the limitation of use also means a limitation of distribution ? For this art. 19(1)(a) and (c): We must insist on taking into account the national

Reference	Third compromise proposal	Drafting suggestion	Comment
			access to public documents regime as was done in PSD2 and in the DGA.
Article 17(3)		[This regulation does not affect the application of national public (access) systems (or records) when it comes to data received under this section.]	One challenge here is that when the right to information is so extensive, it is impossible to assess whether we have sufficient grounds for secrecy to protect this information.
Article 17(4)		'as provided by national law'	What about confidential information and especially e.g. sensitive personal data here ? According to the national doctrine (by our constitutional law committee), provisions on these must be laid down precisely. Thus, it might be necessary to supplement this by the addition "as provided by national law".
Setting up of the dispute settlement bodies			
Article 10		~~If no dispute settlement body is certified in a Member State by [date of application of the~~	Setting up dispute settlement bodies under Chapter III should not be

Reference	Third compromise proposal	Drafting suggestion	Comment
		~~Regulation], that~~ Member State**s** ~~shall~~ **may** establish and certify a dispute settlement body that fulfils the conditions set out in points (a) to (d) of this paragraph.	mandatory. (See ADR directive and DSA art. 18) Justification: We do not oppose the establishment of a dispute resolution body and accreditation here as such. However, the issue for us is, that at least when it comes to ADR-directive, there has been a lack of accreditation applications, and we have appointed the tasks for ADR-bodies that are authorities. We would see it difficult, if we would have to establish such bodies (as envisaged in the data act) for quite 'punctual' new purposes, different from one another, or to pinpoint functions to such existing committees, who do not have the means to handle such issues.
Article 14	Upon request, a data holder shall make data, **which could include**~~ing~~ relevant metadata, available to a public sector	Upon request, a data holder shall make data, including relevant metadata, available to a public sector body or to ~~a Union institution, agency or~~	Comment: the suggested amendment for metadata (as to be provided for optionally) seems a less favourable

Reference	Third compromise proposal	Drafting suggestion	Comment
	body or to ~~a Union institution, agency or body~~ **the Commission, the European Central Bank or Union bodies** demonstrating an exceptional need to use the data requested in order to carry out their legal competencies statutory duties in the public interest	~~body~~ **the Commission, the European Central Bank or Union bodies** demonstrating an exceptional need to use the data requested in order to carry out their legal competencies statutory duties in the public interest	solution than the previous wording. We find this regrettable. This should be 'shall' and not 'could' (or even the previous version 'including relevant metadata'). The addition to art. 17(1)(a) does not appear a full substitute for the loss. Rather, they could even be in contradiction with one-another.
Art. 19(2)		The data holder shall identify the data protected as trade secrets, with relevant mentions/markings in its metadata which are protected as trade secrets.	There should be some (log) entry also into metadata about this.
International data flows			
Article 27		Title: **CHAPTER VII UNLAWFUL ~~INTERNATIONAL~~ GOVERNMENTAL ACCESS AND INTERNATIONAL TRANSFER OF ~~CONTEXTS~~ NON-PERSONAL DATA ~~SAFEGUARDS~~** (1)Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in	Justification: The aim of this article seems to be that Providers of data processing services shall make transparent their policies, practices and arrangements they apply when a request of governmental access to non-personal

Reference	Third compromise proposal	Drafting suggestion	Comment
		order to prevent international transfer ~~or~~ and governmental access to such 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.	data is made. Thus, this might also be stated explicitly (in a recital)
Article 8(1)		**In business-to-business relationships,** where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union 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. - -	Justification: To clarify that B2C relationships are here unaffected
Recital 38		This Regulation contains general **business-to-business** access rules, whenever a data holder is obliged by law to make data available to a data recipient. - -	Justification: To clarify that B2C relationships are here unaffected

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 4(4)		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 and insofar as the disclosure of trade secrets complies with competition law and intellectual property law. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.	To strike a clear balance between promoting innovation and fair access to data and complying with obligations under competition and intellectual property rules.
Article 5(2)			Question regarding the gatekeepers: is the aim here to exclude the entire gatekeeper company or only its core platform service ? (this would affect possibly the ways in which these giants transfer data to their other services for which they have not been designated as gatekeepers).

Reference	Third compromise proposal	Drafting suggestion	Comment
			Question 2: What about the role of consent ? Could a consent be justified for other than core platform services ?
Article 5(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, insofar as the disclosure of trade secrets complies with competition law and intellectual property law. The data holder shall provide such data in the metadata of the data. Such metadata shall not be altered or removed by the user or a third party without the authorisation of the data holder.	

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 6(1)		A third party shall process the data… only for the purposes and under the conditions agreed with the data holder ~~user~~	
Article 6(2)(b)		(The third party shall not:) make the data it receives available to another third party, in raw, aggregated or derived form, unless this is strictly necessary to provide the service requested by the user and provided that the third parties take all necessary measures agreed between the data holder and the third party to preserve the confidentiality of trade secrets identified by the data holder.	
Article 8			Question: what about protective measures ? How to protect IP right ? via technical protection measures or a safe 'channel' ?
Chapter IV			Imbalances in the negotiating power should not lead to circumstances that prevent manufacturers from maintaining and developing safe and secure

Reference	Third compromise proposal	Drafting suggestion	Comment
			functioning of their smart products i.a. prevent use of such data which is essential for diagnostics, research and development and quality control purposes for the manufacturer. (also impacts recital 38).
Article 19(2)		[Suggestion for a new last sentence]The data holder shall identify the data protected as trade secrets, with relevant mentions/markings in its metadata which are protected as trade secrets. The data holder shall provide such data in the metadata of the data. Such metadata shall not be altered or removed by the user or a third party without the authorisation of the data holder.	
Article 31(9) and 32(3)		- - Competent authorities shall, in accordance with Union and national law, respect the principles of confidentiality and of professional and commercial	Articles 31(9) and 32(3) should be further precised (whether /to what extent sensitive or confidential data is processed) and the purpose of the use in these could be stated more precisely.

Reference	Third compromise proposal	Drafting suggestion	Comment
		secrecy and shall protect personal data ~~in accordance with Union and national law~~. Any information exchanged in the context of assistance requested and provided under this Article shall be used only in respect of the matter for which it was requested.	Further, we would also amend the structure in the second last sentence in 31(9) and to change the place of 'in accordance with Union and national law'.
Article 31			We support the idea that regarding the processing of personal data, the competent authority would be legislated at EU-level, in order for the supervision and interpretation to be as uniform as possible.
Art. 31(1)		~~(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, in accordance with national law, of the progress and the outcome of the investigation within a reasonable period, in particular if further~~	The monitoring would (apparently) not be about examining about individual complaints nor publications about them, which is unfortunately how this para. could be understood. Therefore, we request its deletion.

Reference	Third compromise proposal	Drafting suggestion	Comment
		~~investigation or coordination with another competent authority is necessary;~~	
The sui generis database right			
Article 35			Of the two options suggested, FI would prefer option number 1. Question: Is the aim here that the user (of an IoT device) does not have a right to get data In situations where the IoT device presents or confirms the data automatically, without imput of the data holder etc. ? So in cases of algorithmically / electronically/ automatically generated data – so should the data user be able to get this data so the it can provide it to a third party (in order to further develop services based on data)?

Reference	Third compromise proposal	Drafting suggestion	Comment
			See also recital 14a: 'By contrast, information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation. Such data is not generated by the use of the product, but is the outcome of a characterisation, assessment, recommendation, categorisation or similar systematic processes that assign values or insights to a user or product.'
Recital 14			This requires clarification; Art 35 and this recital 14 should be aligned ("collect" .)
Recital 14-a			This requires clarification; 'data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights' would seem (we interpret the

Reference	Third compromise proposal	Drafting suggestion	Comment
			word 'ip' here to refer to software patents. Copyright does not extend to processes. Is that correct ?
Recital 14a			Also this requires clarification in terms of what data is in vs. outside the scope.
Recital 15		Please clarify or delete	The wording as it now stands may exclude some devices outside the scope of the data act which it should not. We are referring here to such devices which are used to presenting but which (users) should get data from. What is more, this recital does not seem to cover services. We hope the Commission could clarify these.
Recital 19			Also this requires clarification; what role does IP refer to here? Copyright protects the use of original works and other protected subject matter; the fact that IP may be involved to protect the content

Reference	Third compromise proposal	Drafting suggestion	Comment
			the product or related service displays/ plays should not limit the users' right to access data produced from the use of the product or service. For instance Spotify should provide the data they collect on the use of the service (what works, how long, when, where from, made by whom…) and when the user is the rightholder, such use is a very important part of achieving full potential of the intellectual property (DSM directive art. 19 Right to transparency). The line between covered products and services would be very difficult distinguish in practise and could be contrary to obligations in other EU legislation and would not benefit the user of the product or service which is the primary aim of this Data Act.

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 2			The compatibility of the definition of smart contract and electronic ledger (art. 2(16) and 2(17)(with the eIDAS-proposal should be assessed. The reference to eIDAS regulation seems to have been removed from art. 2(17).
Article 3		A new last sentence to be added at the very end of article 3: This should be done without endangering their functionality nor going against data security requirements from Regulation 2016/679, product regulations or technical standardisation	
Article 4(3)		Trade secrets shall only be disclosed provided that **the data holder and the user** take all necessary measures in advance **prior to the disclosure** to preserve the confidentiality of trade secrets in particular with respect to third parties. Where such measures do not suffice, the data holder and the user shall agree additional measures, such as technical and organisational measures, to preserve	

Reference	Third compromise proposal	Drafting suggestion	Comment
		the confidentiality of the shared data, in particular in relation to third parties. The data holder shall identify the data, which are protected as trade secrets. The data holder shall provide such data in the metadata of the data. Such metadata shall not be altered or removed by the user or a third party without the authorisation of the data holder.	
Article 5(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. The identity of the data recipient and the scope of data must be disclosed to the data holder for an evaluation of trade secret related risk.	

Reference	Third compromise proposal	Drafting suggestion	Comment
Article 21			We would prefer the Presidency's second option. The data requested (under Article 14) could be shared with research organisations and national statistical institutes (and Eurostat) in accordance with Article 21, and they would be allowed to keep them for additional 6 months after the purpose of the request would be fulfilled. The data would be erased afterwards.
Article 23(1)		Providers of data processing services shall take the measures provided for in Articles 24, 25 and 26 to facilitate customers of their service switching to another data processing service, covering the same type, which is provided by a different service provider. In particular, providers of data processing services shall remove material commercial, technical, contractual and organisational obstacles, which inhibit customers from:	Justification: this could benefit from such a clarification, for more legal certainty

Reference	Third compromise proposal	Drafting suggestion	Comment
		a) terminating the contractual agreement of the service; b) concluding new contractual agreements with a different provider of data processing services; and OR or c) porting its data, applications and other digital assets to another provider of data processing services.	
Article 24		(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 trade ~~business~~ secrets of the provider exists. These exemptions shall however never impede or delay the porting process as foreseen in Article 23;	Justification: 'trade secrets' is already used in elsewhere in the proposal; whereas 'business secrets' is not.
Recital 20		In case several persons or entities **are considered as user, e.g. in the case of co-ownership or when an owner and a renter or lessee exist** ~~own a product or are party to a lease or rent~~ agreement and benefit	See also suggestion in Chapter IV to guarantee subordinate manufacturers and users, to execute their rights and obligations under Data Act. In other

Reference	Third compromise proposal	Drafting suggestion	Comment
		~~from access to a related service~~, reasonable efforts should be made in the design of the product or related service or the relevant interface so that ~~all persons~~ each user can have access to data they generate. Users of products that generate data typically require a user account to be set up. This allows for identification of the user by the manufacturer as well as a means to communicate to exercise and process data access requests. In case several manufacturers or related services providers have sold, rent out or leased products or services integrated together to the same user, the user should turn to each of the manufacturers or related service providers with whom it has a contractual agreement. Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. **Account**	words the rights and obligations of these subordinate users and subordinate manufacturers should not be limited by other manufacturers and users with disproportionate terms of agreements nor with technical means. FRAND terms should therefore apply to all and both ways.

Reference	Third compromise proposal	Drafting suggestion	Comment
		solutions should allow a user to delete their account and the data related to it, in particular taking into account situations when the ownership or the usage of the product changes.	
Recital 28a		-- For this reason, data holders ~~can~~ should be obliged to require the user or third parties of the user's choice to preserve the secrecy of data considered as trade secrets, including through technical means.	Comment: Also the data holders can require that the confidentiality of a disclosure must be ensured by the user and any third party of the user's choice. Quite similarly also in recital 50(a) so here, there would be no obligation – (contractual freedom) ? However, this might be problematic from a trade secret point of view (the criteria for that protection might not be fulfilled).
Recital 29		'A third party to whom data is made available by the data holder may be an enterprise…'	

Reference	Third compromise proposal	Drafting suggestion	Comment
Recital 34		Suggestion for a new wording: In case of also other than personal data: 'In line with the data minimisation principle, the third party should only access additional information [,including personal and non-personal data,] that is necessary for the provision of the service requested by the user. –' Or if this applies to personal data only: 'In line with the data minimisation principle, the third party should only access additional information [,that is personal data,] to the extent necessary for the provision of the service requested by the user. –' And: ' - - Having received access to data, the third party should process it exclusively for the purposes agreed with the user, without interference from the data holder, and take all necessary measures agreed	Comment: We assume that the purpose is agreed upon between the user and the 3rd party.

Reference	Third compromise proposal	Drafting suggestion	Comment
		with the data holder to preserve the confidentiality of trade secrets identified by the data holder. - - '	
Recital 34			Comment: also a third party might 'steer' or guide the use of the data – this should be more strongly reflected in the language here.
Recital 35			Comment: here, it could be clarified whether this applies also to mydata operators, (as only a data intermediation service is mentioned)
Recital 36		[The data made available to the user on basis of the articles 4 and 5 of this regulation may also end up to the competitors of the data holder.] It is important to define the data generated by use in a manner that does not negatively affect competition in the internal market.	
Recital 50a		In order to avoid misuse of the new data access rights, the data holder may apply protective measures, such as technical measures, in relation to	If this recital refers to article 11, the suggestion here would at least make these aligned with one another, because

Reference	Third compromise proposal	Drafting suggestion	Comment
		the data made available to the recipient to prevent unauthorised access and ensure compliance with the framework of data access in Chapter II and III. However, those measures should not hinder…	that article mentions both ”technical protection measures” and ”agreed contractual terms for making data available”.
Recital 56		The notion of data holder other than a public sector body generally does not include public sector bodies. However, it may include public undertakings.	The sentences ‘The notion of data holder generally does not include public sector bodies. However, it may include public undertakings’ need to be clarified.
Recital 66		confidentiality of such disclosure shall be ensured to the data holder.	
Recital 72		This Regulation aims to facilitate switching between data processing services, which encompasses all conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services to port all its digital assets, including data, to the concerned other providers and to continue to use them in the new environment in a way that does not compromise	

Reference	Third compromise proposal	Drafting suggestion	Comment
		innovation and competitiveness of European organisations in the global economy. Digital assets refer to elements in digital format for which the customer has the right of use, including data, applications, virtual machines and other manifestations of virtualisation technologies, such as containers.	
Recital 77		Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested before granting access to that data in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality.	Comment: a challenge is data requests coming from 3rd countries in situations where the data is not protected similarly. The last sentence would need clarification.

Reference	Third compromise proposal	Drafting suggestion	Comment
Recital 80			Comment: Transparency can be ensured in many ways (centralised or decentralised). Question: here, the requirement would not apply to closed systems ? The last sentence about 'can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement' is something which we think could still be clarified.
Recital 82	(82) In order to enforce their rights under this Regulation, natural and legal persons should be entitled to seek redress for the infringements of their rights under this Regulation by lodging complaints with competent authorities. Those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved. In order to make use of the consumer protection cooperation network	- - In order to also make use of the consumer protection cooperation network mechanism - -	

Reference	Third compromise proposal	Drafting suggestion	Comment
	mechanism and to enable representative actions, this Regulation amends the Annexes to the Regulation (EU) 2017/2394 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council.		

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.