ZVEI Recommendations for Amendments to the Data Act Proposal

Introduction

On 23 February 2022, the European Commission published a proposal for a Regulation on harmonised rules on fair access to, and use of, data (hereafter the “Data Act”).

The German electrical and digital industry interlinks with its products and solutions the analogue and digital worlds and is actively shaping this change. Fair access to and use of data is a prerequisite for the digital and green transition of the economy and creates value for society. Therefore, ZVEI believes in the goals set out in the Data Act proposal. However, in order for the Data Act to realize an optimized data allocation a number of uncertainties must be removed.

Our recommended amendments must be read before the background that most legal uncertainties and regulatory obstacles we encounter are caused by the fact that the proposal is based on a very simplified and not practical understanding of the industrial environment. We therefore suggest:

- To foster an optimised data allocation in Europe, the Data Act should support data flows along the entire value chain from TIER 1 to TIER n, also including towards manufacturers that – in fact – do not hold or receive any data that is generated by the use of their products or components.
- Furthermore, Chapter II of the proposal covers both B2B and B2C regardless of different needs in their respective contexts. Thus, legal uncertainties for companies are predetermined. We strongly recommend to separate B2B and B2C data sharing obligation of the Data Act proposal.

With this paper we further build on our previous statements and recommend to EU policy makers some concrete amendments to make the new regulation fit for purpose and make it viable for businesses to thrive in the next phase of the data economy.

The changes in the document compared with the Commission's proposal are **underlined and marked with bold**, deletions with ~~strikethrough~~.

Recommendations for Amendments
Recitals

Amendment 1	
Proposed by the Commission	*ZVEI recommendation*
Recital 15	
In contrast, certain products that are primarily designed to display or play content, or to record and transmit 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, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.	In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, **industrial PCs (including programmable logical controllers),** servers, tablets **(including Human Machine Interface)** and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps. **Overall, existing contracts governing data sharing should be exempted from this Regulation.**
Justification In industrial settings, individual components regularly cannot spontaneously generate data, but rather require a specific and customized configuration by the user or the engineering provider engaged by the user to generate data. Industrial components can only perform their functions based on certain human input configurations by the user. Recital 15 now exempts products which can generate relevant data only on the basis of human input from the scope of the Data Act. Against this background, it would therefore be preferable, for the sake of clarification, that (1) the additional requirement of "human input" is included in the product definition and (2) industrial applications (such as industrial controllers, like "Programmable Logic Controllers" (PLCs), as well as "industrial PCs" (IPCs)) are included in the examples of Recital 15 just like personal computers are excluded from the scope of the Data Act in the B2C environment. Retroactive provisions on data already generated or acquired under existing contracts would impose excessive burden on companies that have placed products on the market before the entry into application of the Regulation, and have contracted related services before that date.	

Amendment 2	
Proposed by the Commission	*ZVEI recommendation*
Recital 23	
(23) Before concluding a contract for the purchase, rent, or lease of a product or the	(23) ~~Before concluding a contract~~ **No later than the moment of delivery - which**

provision of a related service, clear and sufficient information should be provided to the user on how the data generated may be accessed. This obligation provides transparency over the data generated and enhances the easy access for the user. This obligation to provide information does not affect the obligation for the controller to provide information to the data subject pursuant to Article 12, 13 and 14 of Regulation 2016/679.	**represents the fullfilment of the contract** for the purchase, rent, or lease of a product or the provision of a related service - clear and sufficient information should be provided to the user **on its request** on how the data generated may be accessed. This obligation provides transparency over the data generated and enhances the easy access for the user. This obligation to provide information does not affect the obligation for the controller to provide information to the data subject pursuant to Article 12, 13 and 14 of Regulation 2016/679.
Justification In many B2B und B2C relations the customer does not necesseraly have an interest in the information that the manufacturer is obliged to provide by the Data Act Proposal. Also, in case of longer delivery chains through different retailers (in particular small and medium retailers), would not be feasable. Therefore, providing all these information should only be made available on request. Otherwise this provision would create additional and unnecessary administrative burden for the manufacturer and the whole retail chain.	

Amendment 3	
Proposed by the Commission	*ZVEI recommendation*
Recital 24 (NEW)	
(24) NEW	**Where useful, transparency and information obligations should be included in the Digital Product Passport as it will be established in the new Ecodesign for Sustainable Products Regulation (Regulation EC/???). The Digital Product Passport helps consumers and businesses make informed choices when purchasing, renting or leasing products or related services. Existing Digital Product Passport solutions for certain sectors should be considered. For example, in the industry 4.0 area there is a decentralised solution for a digital product passport based on what are referred to sub-models of the asset administration shell (IEC 63278-1).**
Justification We see the potential benefits of the Digital Product Passport (DPP) to guarantee both more transparency along the entire producte life cycle (e.g. product information in re-sale) and easier and secure access to data. We support a decentralised system and a product-by-product approach.In the realm of industry 4.0 the sub models of the asset administration shell enable access to both userfriendly web pages of the manufacturer which may provide all user relevant contract information as well as standardized machine-readable information about the product via a product identification according to IEC 61406 (e.g. in the form of a QR code).	

Amendment 4	
Proposed by the Commission	*ZVEI recommendation*
Recital 60	
For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies and Union institutions, agencies and bodies should rely on their powers under sectoral legislation. This Regulation accordingly does not affect instruments for the sharing, access and use of data in those areas.	For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies and Union institutions, agencies and bodies should rely on their powers under sectoral legislation. This Regulation accordingly does not affect instruments for the sharing, access and use of data in those areas. **In addition, acknowledging the sensitive character of data related to security systems or for the sole purpose of providing security systems service or private security activities, access to data related to security or for the protection of users are not covered by this regulation, especially those that can create a breach of security, including cybersecurity, for a given security system. Therefore, this Regulation shall not apply to situations concerning national security or defence and shall neither affect the collection, sharing, access to and use of data for the sole purpose of providing security services to the user.**
Justification Security systems such as video surveillance systems, access control systems and fire detection systems are used in a wide variety of public environments to protect people as well as property either inside buildings or as part of perimeter protection measures. Allowing access to sensitive data related to such security systems and security systems service has to bear in mind that it can compromise the security of the user, the premises and people in general, and, in fact, the whole performance of the security system/infrastructure itself. Thus, any access to data related to security systems and the provision of security services should be exempted from this regulation.	

Amendment 5	
Proposed by the Commission	*ZVEI recommendation*
Recital 79	
Standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability. In order to facilitate the conformity with the	Standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability. In order to facilitate the conformity with the

requirements for interoperability, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council. The Commission should adopt common specifications in areas where no harmonised standards exist or where they are insufficient in order to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts. Additionally, common specifications in the different sectors could remain to be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. Reusable data structures and models (in form of core vocabularies), ontologies, metadata application profile, reference data in the form of core vocabulary, taxonomies, code lists, authority tables, thesauri should also be part of the technical specifications for semantic interoperability. Furthermore, the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services.	requirements for interoperability, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council. The Commission should adopt common specifications in areas where no harmonised standards exist or where they are insufficient in order to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts. **In contrary, the Comission should consider existing standardisation and semantic interoperability initiatives in certain sectors. In the Industry 4.0 sector, for example, the Asset Administration Shell for industrial applications provides the basis for the development and uns of unified and open Industry 4.0 standards.** Additionally, common specifications in the different sectors could remain to be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. Reusable data structures and models (in form of core vocabularies), ontologies, metadata application profile, reference data in the form of core vocabulary, taxonomies, code lists, authority tables, thesauri should also be part of the technical specifications for semantic interoperability. Furthermore, the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services.
Justification The use of Industrie 4.0 solutions requires interoperability so that components, devices and applications can communicate seamlessly across companies, industries and countries.For more than a decade, the Platform Industry 4.0 has dedicated all its efforts to develop the Asset Administration Shell (ASS) which has made significant progress lately. Companies all around the world adopt the references architectures, standards and norms of the ASS. The Commission should set the right regulatory framework to support the further development and distribution of the ASS:	

Chapter I – General provisions

Subject matter and scope

Amendment 6	
Proposed by the Commission	*ZVEI recommendation*
Art. 1 paragraph 1 & 2 point (a) & (b) & (c)	
1. This Regulation lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest: 2. This Regulation applies to: (a) manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services; (b) data holders that make data available to data recipients in the Union; (c) data recipients in the Union to whom data are made available;	1. This Regulation lays down harmonised rules on making data **that is intended to be transferred, de facto accessible and** generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest: This Regulation applies to: (a) manufacturers **and users** of **connected** products and suppliers of related services placed on the market in the Union and the users of such products or services **when the products or related services obtain, generate or collect data;** b) data holders that ~~make data available to data recipients and~~ **de facto hold, control and are able to grant users** in the Union **access to the data**; (c) data ~~recipients~~ **users** in the Union to whom data are made available;
Justification The data sharing obligation set out in Chapter II of this regulation should apply only to data that is in principle accessible and which is extracted for further use in digital services. Key in the data act is the competition on the digital services level. Leaving any other data in scope would not generate further added value to that goal and create legal uncertainty in relation to IPR/trade secrets, product compliance and contracts. Scope of extracted and already communicated information is dependent on the sector and needs further clarification within these sectors. In complex products , in particular in industrial machines, many data are generated purely to enable the function of the machine by connecting components internally. It must be clarified that these data are not in scope, because the presentation of these data is neither useful nor technically feasible. It must also be avoided that the data-sharing allows full insights in the control mechanisms of the machine. Also, as noted in Recital 17 this Regulation should not	

apply to "derivative data" resulting from a "software process…as such software process may be subject to intellectual property rights." The EC proposal relies on the presumed market asymmetry between the manufacturer or designer of a product (data holder) typically having the exclusive control over the data generated by the use of a product, and the user of that product (data user) who does not have access to that data. In reality, data is extracted by the product manufacturer only if and to the extent stipulated by the contract between the manufacturer and the user and then provided to the user. For this reason, we suggest a more precise definition of "data holder" as the one having the control over the data and being technically and legally able to make it available to the user. This will ensure that the responsibility for ensuring access to data generated by the use of a product will fall on the right actor in the value chain. It is important to add the control-element here, to make it clear that not only manufacturers would be covered by the definition of "data holder", but any other actor who has control over the generated data. This would ensure a more level playing field for data access and truly leverage the EU data economy.

Amendment 7	
Proposed by the Commission	*ZVEI recommendation*
Art. 1 paragraph 4	**Art. 1 paragraph 4**
This Regulation shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 of the European Parliament and of the Council 72 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.	This Regulation shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 of the European Parliament and of the Council 72 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. **This Regulation shall not affect the collection, sharing, access to and use of data generated by security systems or for the sole purpose of providing security systems**

	service or private security activities to the user.
Justification Security systems such as video surveillance systems, access control systems and fire detection systems are used in a wide variety of public environments to protect people as well as property either inside buildings or as part of perimeter protection measures. Allowing access to sensitive data related to such security systems and security systems service has to bear in mind that it can compromise the security of the user, the premises and people in general, and, in fact, the whole performance of the security system/infrastructure itself. Thus, any access to data related to security systems and the provision of security services should be exempted from this regulation.	

Amendment 8	
Proposed by the Commission	*ZVEI recommendation*
Art. 1 paragraph 5 (NEW)	
NEW	**5. This Regulation shall not affect European legislation and national legal acts on the achievement of a high common level of cybersecurity, including the NIS Directive and the Cyber Resilience Act.**
Justification It should be clarified that Union law and respective national legal acts on the achievement of common levels of cybersecurity are not affected by the Data Act	

Definitions

Amendment 9	
Proposed by the Commission	*ZVEI recommendation*
Art. 2 point (1)	
(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;	(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, **as gathered by the source before it has been further processed, cleaned or analyzed;**
Justification One of the core issues with the draft Data Act stems from the vague and broad definitions that it relies on. In practicality this would cause a lot of legal uncertainty for the manufacturers, but also for the users of connected products. For instance, the definition of the term "data" is very broad and needs to be clarified and narrowed down. Understanding the intention of the European Commission appears to be to exclude any "derivative data" from the scope, the term as defined in Article 2(1) should be amended accordingly.	

Amendment 10	
Proposed by the Commission	*ZVEI recommendation*
Art. 2 point (3)	
(3) 'related service' means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions;	'related service' means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing ~~one of~~ **its intended purpose or core** function;
Justification We suggest that the focus of the definition should be on a service being essential for product's 'basic function' rather than 'a function'.	

Amendment 11	
Proposed by the Commission	*ZVEI recommendation*
Art. 2 point (5)	
(5) 'user' means a natural or legal person, including a data subject, that owns, rents or leases a product or receives a related services;	(5) 'user' means a natural or legal person, including a data subject, that **manufactures,** owns, rents or leases a product or receives a related services **and aims to have access to the data produced by the products or services**
Justification The proposal does not provide definitions of the terms "manufacturer" or "service provider" in addition to the terms "data holder", "user" and "data recipient", although manufacturers and service providers are to be equally covered by the scope of the EU Data Act, cf. Art. 1 (2) (a). In general, (component) manufacturers do not play a prominent role in the overall conception of the EU Data Act. They are only required in Art. 3 (2) (d) to provide information on whether they themselves use the data generated by the product they supplied or allow a third party to use the data, stating the purpose for which the data will be used. This particularly shows the proposal's incorrect assumption that, in the industrial sector, the manufacturer of a product is to be qualified as the person who has the ability to make available certain data, i.e., the data holder. On the contrary, the manufacturer and component suppliers are usually cut off from using the data generated by its components products and systems, both technically and due to contractual provisions. In this respect, it proves to be a conceptual gap in the proposal that the manufacturer and the component suppliers are not recognized as having legitimate interests in gaining access to data particularly for the purpose of improving the products, certainly exists in practice and the promotion of innovation and the (further) development of digital and other services is the declared aim of the proposal.	

Amendment 12	
Proposed by the Commission	*ZVEI recommendation*
Art. 2 point (6)	
(6) 'data holder' means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data;	(6) 'data holder' means a legal or natural person who ~~has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data;~~ **de facto holds and controls and is able to grant access to the data.**
Justification The proposal gives the impression of a very simplified and not practical understanding of the relationship between manufacturers and customers in the majority of industrial applications. The proposal does not take into account that in multilateral and multidirectional networks, the "user" of a physical asset is regularly the "data holder". The proposal states in its Explanatory Memorandum that "the manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service" (cf. page 13 of the proposal). However, in most parts of the industrial sector this is not true. The formula "manufacturer = data holder" fails to reflect the realities in the industry environment. Rather, the user typically is the data holder. After delivery of the product or – in more complex systems – its acceptance by the user, the manufacturer of the product does not have access to the data or controls it beyond what has been agreed with the user. The definition of the data holder appears to be at least partially circular, as the proposal itself defines the term "data holder" (i.e., the addressee of the data sharing obligation) as "a legal or natural person who has the right or obligation, in accordance with this Regulation (...), to make available certain data" [cf. Art. 2 (6)]. A more precise definition of the "data holder" is required as the one who de facto holds the data, pointing out that in the vast majority of industrial use cases this role is simultaneously with the user of the component in question. Thus, one-directional horizontal obligations (only manufacturer to user) do not reflect industrial applications and thus seem not to be adequate.- Furthermore the role of "data holder" in many/most industrial sectors is fulfilled by the asset user; it can also be fulfilled by the manufacturer and third party service providers.	

Amendment 13	
Proposed by the Commission	*ZVEI recommendation*
Art. 2 point (12)	
'data processing service' means a digital service other than an online content service as defined in Article 2(5) of Regulation (EU)	'data processing service' means a digital service other than an online content service as defined in Article 2(5) of Regulation (EU)

2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature;	2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature**; SaaS offerings that merely operate on or use rented cloud infrastructures are not data processing services.**
Justification In general, the definition seems to indicate that it is supposed to apply to cloud computing providers such as hyperscalers. However, the definition needs a clearer demarcation as it is unclear whether this applies to manufacturers in cases where they rent cloud infrastructures as a service from a hyperscaler, develop some specific apps for this vendor, and sell these apps as a service to customers. The EU Data Act should not be applicable to these scenarios.	

Chapter II – Business to consumer and business to business data sharing

Obligation to make data generated by the user of products or related services accessible

Amendment 14	
Proposed by the Commission	*ZVEI recommendation*
Art. 3, paragraph 1	
Obligation to make data generated by the use of products or related services accessible 1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use that are accessible 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.	Obligation to make data generated by the use of products or related services accessible 1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use **that are accessible to the data holder and that the data holder controls or uses for their own purposes are**, ~~by default and free of charge~~, easily, **reasonably**, securely and, where relevant and appropriate, directly **(e.g. via web interface**) accessible to the user, in a structured, commonly used and machine-readable format.
Justification In addition, the access by design requirements (Art. 3 No. 1) needs to be specified to ensure that it only covers data that the data holder actually has/controls/uses for his/her won purposes. Otherwise it would impose an undue burden on manufacturers of components, products and systems to make data available that they actually cannot access or have control over. Due to the broad data definition the requirement creates legal uncertainties for the product design process (e.g., which data need to be made accessible). While binding substantial development resources, the access by design requirement creates no value for the data economy. The Commission should do without it. A data sharing obligation that is limited to data that the data holder actually has (as per our proposed amendment to the definition of "data holder") or data	

that the manufacturer uses itself (as notified to the user pursuant to Art. 2 No. 3 (d)) is sufficient to resolve any asymmetrical allocation of data (if any). The Commission should not interfere with the innovative innovation process but leave it to the market participants to decide which data the product generates and makes accessible.

Amendment 15	
Proposed by the Commission	*ZVEI recommendation*
Art. 3 paragraph 2	
2. Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (a) the nature and volume of the data likely to be generated by the use of the product or related service; (b) whether the data is likely to be generated continuously and in real-time; (c) how the user may access those data; (d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used; (e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established; (f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently; (g) how the user may request that the data are shared with a third-party; (h) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31.	2. ~~Before concluding a contract~~ **No later than the moment of delivery which represents the fullfilment of the contract** for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user **on its request**, in a clear and comprehensible format: (a) the nature and volume of the data ~~likely~~ **foreseen** to be generated by the use of the product or related service; ~~(b) whether the data is likely to be generated continuously and in real-time;~~ ~~(c)~~(b) how the user may access those data; ~~(d)~~(c) whether the manufacturer supplying the product or the service provider providing the related service intends to use ~~the~~ **any collected** data itself or allow a third party to use the data ~~and, if so, the purposes for which those data will be used;~~ ~~(e)~~(d) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established; ~~(f)~~(e) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently; ~~(g)~~(f) how the user may request that the data are shared with a third-party; ~~(h)~~(g) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31.

Justification

Ad Art. 3 paragraph 2: In most cases customers are not interested or not aware about data generation. Obligation to inform the customer before signing the contract in any case just complicates process and rise confusion. It should be provided on customer request.Especially in the case of distribution, sell, rent or lease via intermediaries it is not feasible to provide these information at the point of sale (e.g. in the retail shop).

Ad Art. 3 paragraph 2 (b): The information whether data is generated in real-time and/or continuosly has no value to the user but add an unnecessary layer of bureaucratic work to the provider.

Ad Art. 3 paragraph 2 (d): This paragraph bears the risk to completely block any reuse of data by manufacturers and data holders in general and looks likely to significantly disrupt the flow of industrial data across the value chain. It might also pose an obstacle to the manufacturer's ability to collect data from its own products for innovation purposes e.g. to feed and further optimise Artificial Intelligence systems.

Amendment 16	
Proposed by the Commission	*ZVEI recommendation*
Article 3 paragraph 3 (NEW)	
NEW	**3. The manufacturer shall have the right to access easily and securely the data generated by the use of the products it sells, rents or leases.**

Justification

The proposal is based on a very simplified and not practical understanding of the relationship between manufacturers and customers in the majority of industrial applications. The proposal does not take into account that in multilateral networks, the "user" of a physical asset is regularly the "data holder". The proposal states in its Explanatory Memorandum that "the manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service" (cf. page 13 of the proposal). However, in most parts of the industrial sector this is not true. The formula "manufacturer = data holder" fails to reflect the realities in the industry environment. Rather, the user typically is the data holder. After delivery of the product or – in more complex systems – its acceptance by the user, the manufacturer of the product does not have access to the data or controls it beyond what has been agreed with the user.
Component or even full-product manufacturers may not hold or receive by default the data generated through the products they sell. In such cases the user or even a service provider may act as the data holder. To foster an optimised data allocation in Europe, the Data Act should support data flows along the entire value chain from TIER 1 to TIER n, also including towards manufacturers that – in fact – do not hold or receive any data that is generated by the use of their products or components.

Amendment 17	
Proposed by the Commission	*ZVEI recommendation*
Art. 3 paragraph 4 (NEW)	
NEW	**4. Where the user is a legal person, the data holder may seek adequate compensation for making the data accessible.**
Justification There seems to be no reason why access to data would be for free also for users that are legal persons. If the data is co-generated, following Recital 6, then costs for making available should at least be shared in B2B scenarios.	

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

Amendment 18	
Proposed by the Commission	*ZVEI recommendation*
Article 4 paragraph 1	
1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.	1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the ~~data generated by its use of a product or related service~~ **data they control or use for their own purposes** ~~without undue delay~~ **within a reasonable timeframe**, ~~free of charge~~ **for a reasonable fee** and, where applicable **and technically feasible**, continuously and in real-**time in a commercially reasonable manner**. This shall be done on the basis of a simple request through electronic means where technically feasible.
Justification A data sharing obligation that is limited to data that the data holder actually has (as per our proposed amendment to the definition of "data holder") or data that the manufacturer uses itself (as notified to the user pursuant to Art. 2 No. 3 (d)) is sufficient to resolve any asymmetrical allocation of data (if any). he Commission should not interfere with the innovation process but leave it to the market participants to decide which data the product generates and makes accessible.	

Amendment 19	
Proposed by the Commission	*ZVEI recommendation*
Art. 4 paragraph 3	
3. Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.	3. ~~Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.~~ **The data holder is under no obligation to share data that constitute, or allow conclusions about intellectual property and trade secrets of the data holder or third parties.**
Justification Companies shall never be obliged to share trade secrets. Since it is unclear what "necessary measures" mean this article bears the risk that users may impose sharing obligations through the back door.Intelllectua properties and hence trade sectrets is the most valuable source European companies have. It's key to protect rather than risking full access to IP rigts and trade secrets to international competitors. As the recent "Study in the legal protection of trade secrets in the context of the data economy" has shown, the evidence as to whether trade secrets protection facilitates the sharing of data or not remains mixed. Legal and economic uncertainties remain high. European companies need regulations that protects IP rights and thus builds trust in data sharing and foster digital economic growth.	

Amendment 20	
Proposed by the Commission	*ZVEI recommendation*
Article 4 paragraph 6	
6. The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.	
Justification	

We want to raise our concerns that the given wording cause significant uncertainties and therefore ask the co-legislator to clarify the aimed intention. In B2B context, usually manufacturers of IoT assets do not have access to the generated data by default. It is common practice that user generated data is held and can be access by the user. Access and use of data by the manufacturer is realized through contractual agreements. In order to not jeopardizing innovation and data driven growth it is essential that the data act does not create a legal position close to data ownership for the respective user with regard to the use-generated data. We strongly reject the monopolization of data and the creation of new legislation for data ownership rights. Access to and use of data should be organized between partners freely and in fair contracts that take the interests of both sides into account in an appropriate manner. This ensures that customers and business partners can determine and control which data is accessed and for what purpose it is used. However, in particular in B2C context, is must be made sure that Art. 4 paragraph 6 does not create overburden bureaucratic efforts for companies to provide information to their customers that are not necessary or does not create any additional value.

Amendment 21	
Proposed by the Commission	*ZVEI recommendation*
Article 4 paragraph 7 (NEW)	
NEW	**7. Where data holder, manufacturer, and user are legal entities, the access to data shall be based upon a contractual agreement.**
Justification We strongly reject the monopolization of data and the creation of new legislation for data ownership rights. Access to and use of data should be organized between partners freely and in fair contracts that take the interests of both sides into account in an appropriate manner. This ensures that customers and business partners can determine and control which data is accessed and for what purpose it is used.	

Right to share data with third parties

Amendment 22	
Proposed by the Commission	*ZVEI recommendation*
Article 5 paragraph 1	
Right to share data with third parties 1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.	Right to share data with third parties 1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data **they control or use for their own purposes** generated by the use of a product or related service to a third party, **provided that the third party and its ultimate parent companies have their registered seat in the European Union**, ~~without undue delay~~, **within a reasonable**

	timeframe ~~free of charge~~ **, for a reasonable fee** to the user, of the same quality as is available to the data holder and, where applicable **and technically feasible**, continuously and in real-time.
Justification It must be made sure that all obligations on European suppliers, data-holders and manufacturers are only binding to the extent that both the user and any third party involved are located in the EU. Otherwise a significant drain of technological know-how towards competing markets must be feared. Where the actual recipient (third party) is a non-EU organization or is part of a non-EU group of companies, it is likely that restrictions pursuant to Art. 4 (4.) or Art 5(4.) will not be inforced by a third country court.	

Amendment 23	
Proposed by the Commission	*ZVEI recommendation*
Article 5 paragraph 4	
4. The third party shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.	4. The third party shall not deploy coercive means or abuse ~~evident~~ **any** gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.
Justification The misuse of "evident gaps" in the technicial infrastructure might be used as back doors for unlawful behaviour.	

Amendment 24	
Proposed by the Commission	*ZVEI recommendation*
Article 5 paragraph 6	
6. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.	6. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available **by the data holder to the user** where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.
Justification Otherwise inconsistent with the wording of Art.4(4.).	

Amendment 25	
Proposed by the Commission	*ZVEI recommendation*
Article 5 paragraph 8	
8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.	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.~~ **Trade secrets shall not be disclosed to third parties without prior consent by the data holder.** In such a case, **where trade secrests are subject of negotiations,** the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party. **If the data holder and the third party fail to mutually agree on the measures to preserve the confidentiality of the shared data, or data pertaining to other intellectual property rights in scope pf the user request, the data holder shall not be obliged to share such data.**
Justification Companies shall never be obliged to share trade secrets. Since it is unclear what "necessary measures" mean this article bears the risk that users may impose sharing obligations through the back door.Intelllectua properties and hence trade sectrets is the most valuable source European companies have. It's key to protect rather than risking full access to IP rigts and trade secrets to international competitors. As the recent "Study in the legal protection of trade secrets in the context of the data economy" has shown, the evidence as to whether trade secrets protection facilitates the sharing of data or not remains mixed. Legal and economic uncertainties remain high. European companies need regulations that protects IP rights and thus builds trust in data sharing and foster digital economic growth.	

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

Amendment 26	
Proposed by the Commission	*ZVEI recommendation*
Article 6 paragraph 1	
1. A third party shall process the data made available to it pursuant to Article 5 only for	1. A third party shall process the data made available to it pursuant to Article 5 only for

the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose	the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data **without undue delay** when they are no longer necessary for the agreed purpose
Justification To prevent any contractual fraude or missuse of data, third parties must be obliegd to delet received data without undue delay when they are no longer necessary for the agreed purpose.	

Amendment 27	
Proposed by the Commission	*ZVEI recommendation*
Article 6 paragraph 2 point (c)	
The Thrid party shall not: c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;	The Thrid party shall not: c) make the data available it receives to another third party, in raw, aggregated or derived form, unless **(1)** this is necessary to provide the service requested by the user; **and (2) the third party and its ultimate parent have their registered seat in the European Union and (3) are bound by sufficient confidentialy obligations.**
Justification It must be made sure that all obligations on European suppliers, data-holders and manufacturers are only binding to the extent that both the user and any third party involved are located in the EU. Otherwise a significant drain of technological know-how towards competing markets must be feared.	

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

Amendment 28	
Proposed by the Commission +	*ZVEI recommendation*
Article 7 paragraph 3 (NEW)	
3. NEW	3.T**he data holder shall be exempted from the obligations of this chapter, if the product or service is customized to the users' explicit requirements or is a direct result of a development agreement between the data holder and the user.**
Justification Consideration of the specific conditions of B2B-data relationships and B2B-innovation processes: In the B2B-context, machines, systems and data-based services are often developed	

in close cooperation between manufacturers and customers, which require flexibility and often adaptions of and modifications during testing, commissioning and ramping up production. In addition, in particular in the case of smaller companies which are aiming at servitizing their businesses, it might be jeopardizing the digitalisation efforts if data use is exposed to third parties. It is essential that there is still an incentive to invest in data-based services. A temporary protection of investments and development efforts might limit the potentially negative implications on innovation.

Chapter III Obligations for data holders legally obliged to make data available

Conditions under which data holders make data available to data recipients

Amendment 29	
Proposed by the Commission	*ZVEI recommendation*
Art. 8 paragraph 3	
3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, it shall be for the data holder to demonstrate that there has been no discrimination.	3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. **This obligation does not apply to the transfer of data within a legal entity and its subsidiaries.** ~~Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, it shall be for the data holder to demonstrate that there has been no discrimination.~~
Justification Data transfers within a legal entity (e.g. from a local distribution unit to a central processing unit or data unit) shall not be considered as transfers to another data recipient for the purposes of non-discrimination, as the purpose of such an internal transfer has no other market impact as if the data would remain at the same enterprise unit. A proof of non-discrimination would most likely cause the breach of a contractual confidentiality obligation as it would involve the disclosure of the agreements with other data recipients .	

Amendment 30	
Proposed by the Commission	*ZVEI recommendation*
Art. 8 paragraph 4	
4. A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.	~~4. A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.~~
Justification Exclusive agreements are recognized and well-working mechanisms to guarantee that a manufacturer can offer services and products to certain contidtions. They also often form part of long-term agreements where both contractual parties benefit for their own innovation purposes.	

Amendment 31	
Proposed by the Commission	*ZVEI recommendation*
Art. 8 paragraph 5	
5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law.	5. Data holders and data recipients shall not be required to ~~provide~~ **collect** any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law.
Justification This paragraph's intention is misleading as it is unclear to whom the information should not be provided.	

Compensation for making data available

Amendment 32	
Proposed by the Commission	*ZVEI recommendation*
Art. 9 paragraph 4	
4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.	4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail **and in accordance to Art. 101 2008/c 115/01** so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.
Justification	

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

Amendment 33	
Proposed by the Commission	*ZVEI recommendation*
Art. 11 paragraph 1	
1. The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)..	1. The data holder may apply appropriate technical protection measures, ~~including smart contracts,~~ to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1)..
Justification Smart contracts are not an effective means of securing confidentiality of trade secrets. At the time beeing, many of the smart contract proposals that will be discussed have not yet been implemented, or are in a prototype level, and as such their viability is based on nothing other than a few examples that have not been fully tested. In addition, the lack of harmonized standards for smart contracts, undermines interoperability and consequently hinders scaling across industries and borders.	

Amendment 34	
Proposed by the Commission	*ZVEI recommendation*
Art. 11 paragraph 2	
2. A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, shall without undue delay, unless the data holder or the user instruct otherwise:	2. A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed deceptive or coercive means or abused ~~evident~~ gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, shall without undue delay, unless the data holder or the user instruct otherwise:
Justification The wording of "evident gaps" opens the door for potential IP theft attempts and allows the user to instruct the third party on behalf of the data holder, including as regards the IP-protected information. This shall not fall within the discretion of the user, as it is not the IPR holder.	

Amendment 35	
Proposed by the Commission	*ZVEI recommendation*
Art. 11 paragraph 2 point (c) NEW	
Art. 11 (2.) (c) NEW	**2. (c) be held liable for the damages, to the party suffering from the disclosure or breach of contract such as lost profits, royalties and fees which would have been due.**
Justification The remedies for using the provided data for unauthorized purposes or misusing the data otherwise are not proportionate to the infringements and the ensuing damages suffered by the data holder. For instance, if data has been used to develop competing product and the profits have been made, the remedy in the form of destruction of the data would have no effect on the infringing party. End of production, offering etc. would still allow the infringing party to retain the undue profits obtained as a result of the unauthorised use of the data. This calls for the remedies of a deterrent nature and given that the infringements are most likely to affect IP regime and competition law, they shall be based on the remedies typical for these areas of law (cf. the Trade Secrets Directive).	

Amendment 36	
Proposed by the Commission	*ZVEI recommendation*
Art. 11 paragraph 3 point a	
3. Paragraph 2, point (b), shall not apply in either of the following cases: (a) use of the data has not caused significant harm to the data holder;	~~3. Paragraph 2, point (b), shall not apply in either of the following cases:~~ ~~(a) use of the data has not caused significant harm to the data holder;~~ ~~(b) it would be disproportionate in light of the interests of the data holder.~~
Justification The exception in Article 11(3) risks creating legal uncertainty as to what constitutes "significant harm" and what would be "disproportionate" if data were used or disclosed without authorization or prior approval. Any data, that has been obtained based on false information shall be deleted/destroyed immediately. This provision allows for a space where infringement is not only allowed, but almost encouraged given very modest remedies set out in the preceding paragraph. The harm shall be addressed regardless of the damage is has caused, as it often may just depend on the time of discovery, as for instance economic losses are increasing with time passing, thus significance of harm is very relative. In practice, if a wrongdoing is discovered early on, the damage, e.g., making benefits from data made available by the data holder and developing a competing product, making it available on the market, may not yet be significant. However, it will increase with the quantity of sold products and the time going forward.	

Chapter IV Unfair terms related to data access and use between enterprises

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

Amendment 37	
Proposed by the Commission	*ZVEI recommendation*
Art. 13 DELETED	
Art. 13 1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair. 2.	Art. 13 DELETED

A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing. 3. A contractual term is unfair for the purposes of this Article if its object or effect is to: (a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence; (b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations; (c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract. 4. A contractual term is presumed unfair for the purposes of this Article if its object or effect is to: (a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations; (b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party; (c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner; (d) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof; (e) enable the party that unilaterally imposed the term to terminate the contract	

with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so. 5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed. 6. Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding. 7. This Article does not apply to contractual terms defining the main subject matter of the contract or to contractual terms determining the price to be paid. 8. The parties to a contract covered by paragraph 1 may not exclude the application of this Article, derogate from it, or vary its effects.	
Justification The Data Act proposal relies on a presumed market asymmetry between manufacturers or designer of a product and users. This assumption is derived from either just a few industry examples where this can be hold for true or from B2C markets, in particular where few hyberscalers create a de facto oligopol. In the vast mayority of B2B relations, a market or power assymetry or even market failure as described by the comission lacks any empirical evidence. Market participants, even of different sizese can and do negotiate on equal terms. Hence, such an interference with the foundations of the freedome of contract is by no means justified. Furthermore, many contract clauses concerning data sharing cannot be subject of negotiation as specific technical requirements must be given to gurantee the semless function of the product or service. In many business models, access to and make use of user genereted data forms part of the business model. If these specific usage models are up to negotiation, enterprises may not be able to provide their products or services that can compete with international competitors.	

Chapter V Making data available to public sector bodies and union institutions, agencies or bodies based on exceptional need

Request for data to be made available

Amendment 38	
Proposed by the Commission	*ZVEI recommendation*
Art. 17 paragraph 1	
1. Where requesting data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall: (a) specify what data are required; (b) demonstrate the exceptional need for which the data are requested; (c) explain the purpose of the request, the intended use of the data requested, and the duration of that use; (d) state the legal basis for requesting the data; (e) specify the deadline by which the data are to be made available or within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request.	1. Where requesting data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall: (a) specify what data are required; (b) demonstrate the exceptional need for which the data are requested; (c) explain the purpose of the request, the intended use of the data requested, and the duration of that use; (d) state the legal basis for requesting the data; (e) specify the deadline by which the data are to be made available or within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request. (f) be made publicly available online without undue delay **(g) specifiy whether state of the art pseudonomyzation techniques are sufficient.**
Justification The Data Act has the opportunity to finally settle one of the biggest obstacles of industrial data sharing created by the GDPR. There are still considerable uncertainties on the way to (sufficiently) anonymous data and its legal consideration. If the Data Act considers state of the art pseudonomyzation techniques as sufficient this would help European companies to finally make use of data to its full potential.	

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

Amendment 39	
Proposed by the Commission	*ZVEI recommendation*
Art. 19 paragraph 1	
A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 shall: (a) not use the data in a manner incompatible with the purpose for which they were requested;	A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 shall: (a) ~~not~~ solely use the data ~~in a manner incompatible with the~~ **for the** purpose for which they were requested;
Justification The proposed wording is too weak. It must be made clear that the data shall be used soley for the purpose for which it was requested.	

Compensation in case of exceptional need

Amendment 40	
Proposed by the Commission	*ZVEI recommendation*
Art. 20	
1. Data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge.	1. **Any compensation requested by data holders for the d**~~D~~ata made available to respond to a public emergency pursuant to Article 15, point (a), shall ~~be provided free of charge~~ **not exceed the costs directly related to making such data available.**
Justification The effort to provide data can vary substantially depending on the volume, nature, granularity and frequency of access to the data requested by public sector bodies. It is fair that businesses are entitled to recover at least the costs directly related to complying with such request.	

Chapter VI Switching between data processing services

Amendment 41	
Proposed by the Commission	*ZVEI recommendation*
Art. 24 paragraph 1 point b	
(b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;	~~(b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;~~
Justification In the B2C context the information a data holder should provide might hold some valuable information or insights for consumers. However, towards consumers, this would create redundancy with the data privacy information and multiply the length of any terms of use to be agreed with customers. Any change in the service affecting these categories would need a new contractual agreement with the consumer resulting to a fatigue of consumers who be confronted with various updates of terms of use on short intervalls. In the industrial context (B2B), however, the technical and bureaucratic effort to provide the information referred to in Art. 24 (b) is disproportionate to the added value for the user, since neither the user can exploit this information, nor can this information be (meaningfully) used or technically implemented in another platform environment.	

Technical aspects of switching

Amendment 42	
Proposed by the Commission	*ZVEI recommendation*
Art. 26 paragraph 1	
(1) Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall ensure that the	Art 26 (1) DELETED

customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service.	
Justification The definition of "functional equivalence" is too vague. If the Data Act Proposal aims to made provider of data processing services seamlessly transfer the inherint functionalities of their product/service to another provider, this would mean a compelling disclosure of IP and trade sectrets and would prevent innovation eventually.	

Chapter VIII Interoperability

Essential requirements regarding interoperability

Amendment 43	
Proposed by the Commission	*ZVEI recommendation*
Art.28 paragraph 5 (NEW)	
5. The Commission shall, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or in case it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary, with respect to any or all of the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). 6. The Commission may adopt guidelines laying down interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission.	**5. The European Commission shall take into account the standards, good practices, norms and technical specifications which already exist or are being developed in the framework of international and European standardisation organisations as well as sectorial European Joint undertakings working of data-sharing standardization.** ~~5~~. **6.** The Commission shall, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or in case it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary, with respect to any or all of the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). ~~6.~~**7**. The Commission may adopt guidelines laying down interoperability specifications for the functioning of common European data spaces, such as architectural models

	and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission.
Justification We fully supports the objective under Chapter VIII to pursue standardisation efforts in the field of interoperability to realize the objectives of the Data Act. We strongly recommend that any new process aiming to develop open interoperability specifications and/or European standards on interoperability should take into account existing industry-driven practices.	

Essential requirements regarding smart contracts for data sharing

Amendment 44	
Proposed by the Commission	*ZVEI recommendation*
Art. 30	
The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties; (b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions; (c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and (d) access control: a smart contract shall be protected through rigorous access control	The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: (a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties; ~~(b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;~~ ~~(c)~~ **(b)** data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and ~~(d)~~ **(c)** access control: a smart contract shall be protected through rigorous access control

mechanisms at the governance and smart contract layers.	mechanisms at the governance and smart contract layers.
Justification The obligation of "safe termination and interruption" contradicts the contemporary technical definition of smart contracts. Art. 30 b would alter the legal basis for millions of smart contracts in place and important innovation such as in selfgoverned identities or decentralized platforms which are governed by smart contracts would be prevented.	

Chapter X Sui generis rights under Directive 1996/9/EC

Amendment 45	
Proposed by the Commission	*ZVEI recommendation*
Art. 35	
In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.	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 **these particular parts or sets of** databases containing data **directly** obtained from or generated by the use of a product or a related service.
Justification In order to maintain the principle of proportionality it must be specified that only those parts of a database are affected by this article that demonstrably contain data that have been directly generated by the use of a product or a related services.	

Chapter XI Final provisions

Entry into force and application

Amendment 46	
Proposed by the Commission	*ZVEI recommendation*
Art.42	
This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from [12 months after the date of entry into force of this Regulation].	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from [~~12~~ **36** months after the date of entry into force of this Regulation].
Justification The transition period of 12 month is too short, in particular when considering both necessary product design obligations for connected products under Art. 3(1) adjustment and redesings as which will require from companies analysis, important decisions on their business models, and then adaptation of their manufacturing processes well as the fact that technical requirements for interoperability in EU data spaces are yet to be developed.	

Contact

Dominic Doll • Manager Digitalisation and Innovation Policy • Digitalisation and Innovation Policy Dep. •
Tel.: +49 30 306960 19 • Mobile: +49 151 26441 132 • E-Mail: Dominic.Doll@zvei.org

ZVEI e. V. • Electro and Digital Industry Association • Charlottenstraße 35/36 • 10117 Berlin • Germany
Lobbying Register ID.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

Date: October 17, 2022