ZVEI key recommendations on the Data Act's Trilogue negotiations

In this document we address the most important amendments to the Data Act Draft for the Electro and Digital Industry as seen in the 4-column document from June 13th. This document built upon our extensive ZVEI recommendations to the Data Act Draft.

Content

Key recommendations

The **protection of sensitive information, including trade secrets and security and cyber relevant data** is still of utmost importance to the electro and digital industry in the ongoing Trilogue negotiations. The threat of a drain on business know-how, combined **with technically and legally unclear definitions** (especially 'related service', 'data holder') and the **cascade of new definitions** as seen in the latest 4-column document ('product data', 'related service data') is **creating legal uncertainty across the industry** and thwarts the Commission's policy objective of improving EU's data market.

In order to achieve the politically intended balance between preserving incentives to invest in innovation on the one side and creating new innovation opportunities through an improved distribution of the value from data sharing towards users and third parties on the other side, **effective ex-ante AND ex-post measures to protect trade secrets and intellectual properties in B2B, B2C and B2G relationships** must be taken. Trade secret holders must have the right to **reject a data sharing request ex-ante** insofar the protection of sensitive information is affected, and the trade secret holder can demonstrate – based on transparent and detailed justifications – why a data sharing request is to be rejected. This applies regardless of whether the user or third party is a natural or legal person located either in the EU or a third country.

ZVEI recommends that the Data Act allows for a **longer transition period, of at least 36 months**, to give companies from all sectors time to prepare and comply with the Data Act. It should also be considered that product development cycle in industrial settings takes on average 4-5 years.

How to read this document:

Green: Is what has been agreed on technical level as far as known.

Yellow: Article is still negotiated on technical level and is likely addressed on political level. We highlight those proposed Amendments that we deem most useful and to consider in further discussions OR that need to be urgently re-drafted or deleted.

Definitions

	EU Data Act proposed Amendments	ZVEI Recommendations
	‘**readily available data’** Art. 2 para 1 (1e)	
	‘readily available data’ means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort, going beyond a simple operation;	The introduction of the new definitions ‘readily available data’, ‘product data’ and ‘related service data’ do not serve to create more clarity. Quite the opposite is the case. The Data Act should provide definitions that set a clear scope. The newly introduced definitions form a chain of references that ultimately leads back to the original term of ‘data generated by the use of a product’, which, however, is still not conclusively defined.
	‘product data’ Art. 2 para 1 (1f)	
	‘product data’ means data, generated by the use of a connected product, that the manufacturer designed to be retrievable, via an electronic communications service, a physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.	
	‘**related service data’** Art. 2 para 1 (1fa)	
	‘related service data’ means data representing the digitization of user actions or events related to the connected product, recorded intentionally by the user or as a by-product of the user’s action, which is generated during the provision of a related service by the provider;	
	‘connected product’ Art. 2 para 1(2)	
	‘connected product’ means an item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate product data via an electronic communications service, a physical, connection or on-device access and whose primary function is not the storing, processing or transmission and processing of data on behalf of third parties, other than the user;	We strongly recommend considering following amendments: ‘connected product’ means an item, that ~~obtains~~, generates ~~or collects~~, data concerning its use or environment **and which is accessible by data holders by means of a simple operation**, and that is able to **directly** communicate product data via an electronic communications service, a physical, connection or on-device access and whose primary function is not the storing, processing or transmission and processing of data on behalf of third parties, other than the user; **Justification:** • "Obtains" and "collects" should be deleted to clarify the scope of the definition in the

		context of multiple products working in the same IoT network. Products would fall under the Data Act only insofar as they "generate" data. In IoT networks several products may be obtaining/collecting data from others, in which case all those products would fall under the Data Act obligations to share the same datasets. Instead, in the context of IoT networks, it seems more logical to determine which product generates which dataset. Therefore, limiting the scope to data "generation" would help to distinguish which product of the network must make available which data. • In the second indent, the scope should be limited to "direct" communication. The Council's suggestion to include "indirect" communication is unclear and would lead to legal ambiguity.
	'related service' Art. 2 para 1 (3) (from: **Council Amendment**)	
	'related service' means a digital service other than an electronic communications service, including software, which is connected with the product at the time of the purchase in such a way that its absence would prevent the product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the product;	This new definition disproportionately expands the scope of the Data Act as manufacturers are obliged to design the products with an accessibility of data by design and thus an unpredictable scope of data would be exposed.
	'data holder' Art. 2 para 1 (6) (from: **Council Amendment**)	
	'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, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;	The draft agreement of the definition "data holder" shows some improvements as it considers industrial practices and realities where the manufacturer of an IoT asset is not necessarily the holder of the generated data. However, it should be clarified that being a data holder requires both data access **AND** data control (contractually agreed right to use such data). Otherwise, manufacturers that have ceded the right of data access and use to the user (which is common in industrial sectors) would be covered by the definition.
	'trade secret' Art 2 para 1 (20e)	
	'trade secret' means information which meets all the requirements of Article 2, point (1) of Directive (EU) 2016/943;	We welcome the clarification and that the term "trade secret" has been defined.
	'trade secret holder' Art. 2 para 1 (20f)	
	'trade secret holder' should be understood as per Article 2, point (2) of Directive (EU) 2016/943.	To avoid legal uncertainties and reflect industrial realities it is essential to introduce the notion of "trade secret holder", in

		accordance with the Trade Secrets Directive 2016/943. A data holder is not always the trade secret holder!

Protection of security-relevant data

EU Data Act proposed Amendments	ZVEI Recommendations
Art. 4 para 1c (From: **EP Amendment**)	
Users and data holders may agree contractually on restricting or prohibiting the access, use of or further sharing of data, which could undermine security of the product as laid down by law. Each party may refer the case to the data coordinator, to assess whether such restriction is justified, in particular in light of serious adverse effect on the health, safety or security of human beings. Sectoral competent authorities will be given the possibility to provide technical expertise in this context.	We welcome the acknowledgement of the European Parliament that in exceptional situations, in particular where the security of a product is concerned, data holders are not obliged to make available data. However, we believe this article needs to be strengthened to deploy its full potential: - Instead of making the protection of highly sensitive data dependent upon an agreement between data holder and data user, the data holder should have the possibility to "restrict or prohibit the access, use of or further sharing of data, which could undermine security of the product" - This principle should be incorporated not only in Art. 4, but also in Art. 3 and 5. **Justification**: Certain data are particularly sensitive and linked to the core internal functioning of the product and its interplay with other (sub)-systems. Inappropriate use of such data can expose the product's vulnerabilities to malicious actors and create security risks. We therefore support that there needs to be a possibility for the data holder to deny access to data where product's security, safety and human health are concerned. We believe that by allowing the data user to challenge the decision by the data holder and the involvement of sectoral authorities, the provisions guarantee a proportionate application of such exception.

Data sharing along the entire value chain

EU Data Act proposed Amendments	ZVEI Recommendations
Art. 4 para 6a & 6b (From: **EP Amendment**)	
~~6a. Data holders shall not make available non-personal data accessed by them from the connected product, referred to in point (a) of Article 3(2), to third parties for commercial or non-commercial purposes other than the fulfilment of their contractual obligations to the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.~~ ~~6b. Where the contractual agreement between the user and a data holder allows for the use of non-personal data accessed by them from the connected product, referred to in point (a) of Article 3(2a), the data holder shall be able to use that data for any of the following purposes:~~ ~~(a) improving the functioning of the connected product or related services;~~ ~~(b) developing new products or services~~ (c) ~~enriching or manipulating it or aggregating it with other data, including with the aim of making available the resulting data set to third parties, as long as such derived data set does not allow the identification of the specific data items transmitted to the data holder from the connected product, or allow a third party to derive those data items from the data set.~~	We strongly support DELETING the proposed Amendment and stick to the Commission's initial proposal of Art. 4 para 6. **Justification:** The first sentence of Art 4(6) already gives data users all possible rights to determine what will happen to their data. This paragraph even prohibits the user from agreeing that data holders can re-share users' data with third parties behind compensation. Art 4(6) is sufficient to leave them that contractual freedom. This paragraph would prevent the data holder and its partners, for instance component or material suppliers, from using the data for general and nonuser-specific R&D purposes, resulting in less innovation and poorer product performance which are not in the interests of users and the wider industrial ecosystem. There are no visible grounds to prescribe the range of possible data re-use by law in Art. 4 para.6b. Innovation in the data economy is fast and will bring new models which may not appear in this list, resulting in a weakening of European innovation .. Article 4(6) is already sufficient to base data re -use on the user's consent if that is the purpose.

Trade secret protection between data holder and user

	EU Data Act proposed Amendments	ZVEI Recommendations
	Art. 4 para 3	
	Trade secrets shall be preserved and shall only be disclosed provided that the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular with respect to third parties. The data holder [or the trade secret holder when it is not the same legal person as the data holder] shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the user proportionate technical and organisational measures necessary to preserve the	For a reliable protection of trades secrets, we believe further improvements still need to be made: - As mentioned above, it is essential to introduce and define the notion of "trade secret holder", in accordance with the Trade Secrets Directive 016/943 to avoid legal uncertainties.

	confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.	
	Art. 4 para. 3a	
	Where there is no agreement on the necessary measures or if the user fails to implement the agreed measures or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing without undue delay to the user. In such cases, the data holder shall notify the [data coordinator/national competent authority] designated in accordance with Article 31 that it has withheld or suspended the sharing of data and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality compromised.	- Trade secret protection needs to be ex ante as established under the Trade Secrets Directive. - In case no agreement can be reached between the data holder and the user data sharing should not commence. This paragraph is only an improvement towards more reliable trade secrete protection only it is supplemented with the ex ante right to refuse the data sharing from Art. 4 para 3c.
	Art. 4 para. 3b	
	Without prejudice to the user's right to seek redress at any stage before a court or a tribunal of a Member State, the user wishing to challenge the data holder's decision to withhold or suspend the sharing of data may: - lodge in accordance with Article 31(3), point b), a complaint with the [the data coordinator/national competent authority], which shall, within a reasonable period of time, decide whether and under which conditions the data sharing shall start or resume; or - agree with the data holder to refer the matter to a dispute settlement body in accordance with Article 10(1a).	
	Art. 4 para. 3c (From: Council Amendment)	
	In exceptional circumstances, when the data holder can demonstrate that it is highly likely to suffer serious damage from the disclosure of trade secrets , despite the technical and organisational measures taken by the user, the data holder may refuse the request for access. Such demonstration shall be duly substantiated, provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.	While the Council foresees the possibility of an ex ante right to refuse data sharing – which we highly welcome – the threshold for the data holder to invoke this right is too high as it is limited to situations where there is a risk of bankruptcy of the data holder or similar grave threat to an entities' viability. Instead "serious damage" – as referred to in Recital 28a - should refer to 'the economic harm to the data holder which may result directly from the disclosure of the data holder's or its suppliers trade secrets, for example where access to such data leads or may lead to the critical device know-how being disclosed such as in relation to interfaces and interactions between internal components or sub-components of the system or contributes significantly to the infringement of the data holder's intellectual

		property rights, including through reverse engineering.' This would reflect goals of Data Act stated in recital 28a.

Trade secret protection between data holder and third parties

	EU Data Act proposed Amendments	ZVEI Recommendations
	Art. 5 para 8	
	Trade secrets shall be preserved and 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. The data holder [or the trade secret holder when it is not the same legal person as the data holder] shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the third party all proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct	In general, we welcome that the level of trade secrets protection towards third parties have been aligned with Art. 4 para 3. For further improvements please refer to the recommendations above. •
	Art. 5 para. 8a (From: Council Amendment)	
	In exceptional circumstances, when the data holder can demonstrate that it is highly likely to suffer serious damage from the disclosure of trade secrets , despite the technical and organisational measures taken by the user, the data holder may refuse the request for access. Such demonstration shall be duly substantiated, provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.	While the Council foresees the possibility of an ex ante right to refuse data sharing – which we highly welcome – the threshold for the data holder to invoke this right is too high as it is limited to situations where there is a risk of bankruptcy of the data holder or similar grave threat to an entities' viability. Instead "serious damage" – as referred to in Recital 28a - should refer to 'the economic harm to the data holder which may result directly from the disclosure of the data holder's or its suppliers trade secrets, for example where access to such data leads or may lead to the critical device know-how being disclosed such as in relation to interfaces and interactions between internal components or sub-components of the system or contributes significantly to the infringement of the data holder's intellectual property rights, including through reverse engineering.' This would reflect goals of Data Act stated in recital 28a1 .

Entry into force

	EU Data Act proposed Amendments	ZVEI Recommendations
	Art. 42 para. 2 (From: **EP Amendments**)	
		Regarding the entry into force provision (Art. 42), we see a need for urgent improvement in both EP's and Council's position. We strongly recommend setting a transition period of at least **36** months for all provisions. **Justification:** Existing contracts and products already placed on the EU market should be grandfathered – meaning that the obligations under Art. 3-5 shall only apply to products placed on the market after the date of application of the Regulation. It is also essential that the transition period is extended to provide manufacturers with the possibility to comply with the Data Act because the product development cycle in industrial settings takes on average 4-5 years.

Contact
Dominic Doll • Manager Digitalisation and Innovation Policy • Department Digital and Innovation Policy•
Tel.: +49 30 306960 19 • Mobil: +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: June 16, 2023