bitkom

Bitkom Position Paper EU Data Act Proposal

April 19, 2022

Long version

bitkom

Content

bitkom

Bitkom welcomes the European Commission's Data Act proposal (the Data Act) and its intention to increase the breadth and depth of data usage and innovation within the European Single Market as this will help to fuel the digital transition by offering countless new opportunities to European citizens and businesses.
In the following, we provide general remarks, also on individual chapters, and then comment on specific elements of the Data Act.

General remarks

From an overarching perspective, we would prefer the regulation allow sufficient room for the fundamental principles of the market economy to develop, particularly in still *nascent* markets such as for the sharing of data. Here and there, we are rather reminded of market design than of regulatory interventions to address market failures. **In that sense, we are rather uncertain about particular propositions including but not limited to mandatory data sharing with other businesses, essentially extending transparency obligations to B2B settings, as well as unequal treatment of market participants (micro, small, and medium enterprises, corporates) in some circumstances. Generally, provisions should be drafted in a manner in which companies of any size can easily fulfil them.**

Nevertheless, we do also recognize the potential benefits of data sharing and the determination of the Commission to move forward with this Regulation. Thus, we are eager to engage in a constructive dialogue to make the proposed rules work best by specifying and amending them where appropriate.

Clarifications are needed to ensure the primacy of the GDPR[1], and compatibility with new provisions under the Data Act. In particular, the Data Act has a potential influence on the personal data processing chain and the consideration such processing is necessary for the purposes of the legitimate interests (Art. 6 para 1 pt. f GDPR), which would merit more clarity.

In all circumstances, full respect of trade secrets, intellectual property, reasonable compensation, and other applicable laws should be paramount. This approach concerns users and data holders as well as other companies in the value chain. In order for this approach to enable innovations that are not yet foreseeable or plannable today, we believe the proposal needs to provide clearer limits on the development of a competing product by third parties.

While we acknowledge the difficulty in distinguishing trade secrets from other types of (IP) information on an objective basis across EU members states, we are strongly concerned about insufficient safeguards to protect trade secrets in the Data Act

[1] Regulation (EU) 2016/679

Berlin,
April 19, 2022

Bitkom e.V.

David Schönwerth
Policy Officer Data Economy
T +49 30 27576-179
d.schoenwerth@bitkom.org

Rebekka Weiß, LL.M.
Head of Trust & Security
T +49 30 27576-161
r.weiss@bitkom.org

David Adams
EU Public Policy Officer
T +49 30 27576-585
d.adams@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Given the absence of an objectivity test regarding the classification of information as trade secrets in certain member states – also following the transposition of the EU trade secrets directive, trade secrets should be excluded from data sharing obligations, be it even with a corollary objectivity criterion as already implemented in certain member states following the transposition of the EU trade secrets directive[2], in any case, the Data Act should be clearer on the nature of the specific measures necessary to preserve the confidentiality of trade secrets. Moreover, there should be clear rules on third party liability in the case of unlawful disclosure of trade secrets under the Data Act.

In addition, there is a lack of (concrete) provisions regarding information security during and after the sharing of sensitive information. Apart from that, rules concerning data storage (e.g., duration, addressee, storage location) would merit more clarity. In light of various affected verticals, it must be ensured that elementary/basic technical implementations (e.g., due to cyber security reasons) are not negatively affected. The data sharing to user/third party must not become a gateway for criminals, so that the security/safety/privacy of the user is endangered. This can include but is not limited to direct attacks or illegitimate insights into capabilities of companies or verticals.

Interaction with current and future legislation

We suggest to further clarify and align the relationship with the AI Act[3] under negotiation, announced or proposed sectoral initiatives concerning data sharing, the GDPR, the existing e-Privacy Directive[4], the upcoming e-Privacy Regulation[5], the upcoming Digital Markets Act[6] as well as (MS-level) legislation on confidentiality of information flows.

Generally, we support, that the EU Commission intends to address certain markets and their dynamics. The Data Act is meant to be a horizontal instrument, which is why we believe that, generally, there should be no unequal treatment between SMEs and non-SMEs in most circumstances. For example, current provisions in force regulating unfair terms between companies generally do not take size into account either. Instead, a level playing field together with easier implementable rules for all would be the ideal outcome and create more clarity.

[2] Directive (EU) 2016/943
[3] COM/2021/206 final
[4] Directive 2002/58/EC
[5] COM/2017/10 final
[6] COM/2020/842 final

Regarding the references to future gatekeepers in the Digital Markets Act in Chapter 2, we would like to point to our five principles for a functioning Digital Economy and fair competition:[7]

- Retain core competition mechanics: Scope should be based on objective evidence,
- Taking diversity into account: Obligations should not follow a one size fits all approach,
- Reliable rules: Application and rules must be clear and tailored,
- Ensure innovations in Europa: Justifications and procompetitive behavior needs to be preserved,
- Market investigations: Clarifying scope and purpose.

Chapter 2 – IoT Data Sharing

We welcome the European Commission's objective to facilitate data sharing for IoT devices and related services. We believe that better transparency and access to data generated by users can enable a more competitive aftermarket including through the generation of new innovative business models and solutions.

> Data sharing obligations must not have a prohibitive effect and deter companies from offering IoT solutions.

It is critical that **data sharing obligations do not have a prohibitive effect and deter companies from offering IoT solutions** (be it products or services) in the first place. Here, it should be recognised that in-fact, data is often rivalry as it carries potential and actual economic value – else data sharing would not be up for debate.

Gradually, holding data turns into a legal and competitive risk especially for SMEs while the use of many types of data by them is not always market reality. In the same manner, increasing compliance cost might actually backfire when it comes e.g., to B2B data sharing.

The prohibition to use the data received from the data holder for the development of a competing product should, in our opinion, not only apply to products, but also to related services. There is no obvious reason to restrict the scope of Art. 6 para 2 pt. e to products only while data can also be obtained from related services.

It is important to state that a prohibition to compete with the product or related service that the data originated from does in no way prevent a third party from offering an (aftermarket) service that may be in competition with a product or related service other than the one the data originated from. Hence, the pro-competitive effect of the Data Act would be maintained.

Since we observe quite intense discussions regarding horizontal and/or vertical rules, we would like to present a way forward which accounts for consumer protection, innovation, as well as increased data usage in various fields at the same time. In

[7] https://www.bitkom.org/sites/default/files/2021-03/20210315_-bitkom-principles-digital-markets-act.pdf

principle we support the EU Commission's approach of facilitate to and use of data to boost Europe's competitive advantage as well as ability to innovate.

Regarding personal data, such could be made available to all interested market participants in anonymised form if this is sufficient to meet the user's needs and the legal prerequisites are fulfilled for such data processing and sharing.

Regarding non-personal data, a more restrictive access to data, differentiation between types of data and strong protection of trade secrets is needed. Machine data without personal reference should not be made accessible across the board to all eligible market participants. Instead, a balance that still encourages the development and monetization of services should be found. Reasonable compensation for data holders should be possible in general to grow the data economy and provide incentives. Else, such provision would discourage new data-based additional services for IoT assets as providers might not be incentivized to develop such in the first place. In particular, we suggest narrowing the scope product functions (back) to core functions. Else, virtually any type of related service would be included from any actor.

Reasonable compensation for data holders should be possible in general to grow the data economy and provide incentives.

Above approach would obviously leave certain points up for discussion, in particular conflicts of interests when it comes to determining which data represents personal data and which does not, as this question will also influence the implementation of the Data Act. However, solving this question is of highest urgency in any event and thus will only receive further attention, which we welcome.

Similarly, remaining uncertainty about what constitutes **legally effective anonymization** is an important issue, leading to legal uncertainty and potentially expansion of the existing *GDPR-uncertainty* to non-personal data. As a side note, within the scope of GDPR and Data Act, we also note remaining uncertainty about what **legally effective pseudonymization** constitutes.

As long as there is no clear distinction between personal and non-personal data in practise, some would be tempted to construct the existence of personal data, counteracting the intention of the Data Act to complement the GDPR Art. 20 portability rights for third parties with the consent of consumers and moving everything under the GDPR regime. For example, it could be argued that telemetry data of a technical system has different characteristics due to different operating personnel, making the personnel identifiable from the telemetry data, potentially with the help of staff schedules.

Furthermore, the precise mechanism between Art. 20 GDPR portability rights on the one hand and Art. 4 and 5 portability rights of the EU Data Act, needs to be further clarified. This also applies to access rights in settings where a third data subject may be involved.

Regarding other points for improvement, we see **potential for further clarification regarding the distinction between data holder, user, and data recipient**. For example, the IoT asset provider is not always the data holder as assumed by the Data Act.

Instead, the customer who uses the device in fact holds the data, which should be acknowledged in defining obligations for data holders.

Similar questions arise where direct relationships are absent between parties such as in product rental contracts between OEM and user where obligations for OEMs are unclear or impossible to fulfil. It should also be noted that the allocation of duties under the Data Act depends heavily on the legal construction. An example:

- An OEM builds a machine that is classified as a product
- An investor buys the machine and leases it to a producer
- The producer uses this machine in its production
- The technical maintenance is contracted out to a partner company of the producer
- The IT-technical supervision is contracted out to another specialized company.

Depending on how the contracts are structured and on the ownership of the sensor technology, each of the players could be a user or data owner. At the same time, the constellation of such a construct (i.e., many bilateral contracts) is hardly understandable and actionable for a single company.

Regarding the aforementioned points on trade secrets, especially in Chapters 2 and 5, we see the risk of (mis)classification of information. A possible example is telemetry data which we believe is usually not regarded as a trade secret. Sharing such data with possible competitors or other market participants in general could enable the profiling of companies or whole verticals by various actors e.g., for potential acquisitions or other purposes, which has to be addressed.

Moreover, the Commission explicitly refers to diagnostics data as data that users should be able to share with third parties. Such information is oftentimes unstructured and as such very difficult for users to understand and therefore difficult to manage. If users would now be incentivized to share such data with a third-party, the information could be easily abused by bad actors who could potentially analyse and use it for purposes that users were not aware of or could potentially find ways to hack the devices and thereby undermining the users' overall security.

We also miss clear and market-applicable distinction between data under the scope of the Data Act and configuration data. In any event, it is essential that the data holder can claim damages from the originator (i.e., the user or data recipient) if their data has been misused - e.g., for the development of a competing product. The right to a mere deletion of the data does not seem sufficient. **What's missing further is a clear provision in terms of liability if data is misused.**

Chapter 3 – Obligations

We consider the scope of the companies defined as micro, small or medium enterprises in Art. 9 too extensive. In effect, in case of mandatory data sharing, only data shared from micro, small or medium enterprises vis-à-vis large companies would

allow for making a profit, whereas all other constellations would only be allowed to cover cost.

In particular, it seems problematic that such provision would also apply to micro, small or medium enterprises acting as data holders themselves, with the effect that such firms could not make any profit from data sharing anymore from trading with other such companies, e.g., another SME. **In other words, data sharing between small, micro, or medium enterprises would be limited to cost-only pricing and hamper growth of micro, small and medium enterprises significantly.** Ironically, SMEs would potentially find themselves confronted with a ban on profits, high costs, little utility, ambitious legal and technical requirements, without necessarily a respective business model to use such data, which could render potential gains of Chapter 3 to large players only. Rather, Art. 9 para 1 would suffice to prevent unreasonable margins for all market participants but still would merit more clarity to actionable.

Furthermore, Art. 11 in its current form falls short of being an effective deterrent of unauthorized use or disclosure of data as the user may instruct an infringing data recipient not to take any steps.

Chapter 4 – Unfairness Test

The provisions in Art. 13 seem to conflict with the established provisions on control of contents in general terms and conditions in the Civil Codes of (certain) EU Member States. Therefore, there is no necessity for further regulation on EU level; if any, we see the occasion for **voluntary alignment on the national level.**

We do not see why large companies could not suffer from contractual imbalances given their size, this seems to be a matter of specific circumstances relating to buying power, substitutability, and overall diversity of supply.

Chapter 5 – B2G Data Sharing

In recent years, businesses have successfully proven their willingness for cooperation with public sector bodies in case of public emergencies which could well prevail. Thus, the Data Act should not neglect incentivising and fostering voluntary B2G data sharing. In the EU, there are many examples of successful B2G data sharing initiatives in place, as the B2G Data Sharing report from the Commission's Expert Group rightly outlines.[8] In the context of the Covid-19 crisis many more examples can be added to this list. The reaction towards the pandemic has shown that, once the purpose of sharing data is clearly outlined, the willingness to share data increases significantly. These positive examples highlight the potential of voluntary cooperative data exchanges between the private and public sector, as they are faster and less bureaucratic.

The Data Act should not neglect incentivizing and fostering voluntary B2G data sharing.

[8] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

We struggle to identify an addressable market failure for the cases related to public emergencies (Art. 15 pts. a, b)[9] that would justify such broad and horizontal intervention. In addition, the current text could lead to unintended consequences.

The proposal does not seem to take into account fairness, transparency, reasonableness, and non-discrimination and doesn't include sufficient safeguards for privacy, security, protection of business secrets and IP.

Today, there are many risks and barriers that hinder the benefits of voluntary data sharing from being realised. The Data Act unfortunately is not addressing this issue. A crucial barrier for data sharing is the often very high ex-ante cost associated with it. While we generally welcome the possibility to receive compensation for sharing certain data in the Data Act, putting in place attractive compensation mechanisms or simply commercial data acquisition / licensing agreements for companies could be a more efficient way to achieve the desired objective. These incentives could be direct (e.g., monetary) or indirect (e.g., reputational).

In any event, we miss a more narrowly, explicitly, and precisely defined scope of the covered data as well as a set of scenarios under which mandatory B2G data sharing would be required as a last resort, including a clear definition of public interest. As it stands, the notion of public interest could cover anything from traffic management to statistics. If such a category is included in the final act, the term "public interest" needs to be narrowly defined within the act itself to avoid legal uncertainty. It also needs to be clear where the lack of data would prevent a public sector body from fulfilling a task in the public interest.

Also, the definitions of public emergencies and exceptional need appear overly broad and thus open ways for interpretation and abuse of this right. The reference made to "major cybersecurity incidents" in Recital 57, for example, raises serious questions as to the exceptional nature of such emergencies. The public sector access to private sector data is also foreseen for prevention and recovery from public emergencies. However, it is not stated what prevention and recovery actual means. Clarification is necessary that not every circumstance can be framed as prevention or recovery.

Additionally, the Data Act seems to fall short of sufficient technical and non-technical safeguards for information security before, during and after data sharing with public sector bodies. Here, both the capability of public sector bodies to securely handle data as well as their ability to process potentially vast amounts of data effectively and efficiently should be ensured. Transparency obligations should oblige governments and public administrations to report to the company how the data requested was used to limit excessive requests and to enable companies to review that the obligations according to Art. 19 were indeed met by the requesting public sector body.

[9] Art. 15 pt. c 1 includes a market failure test to some extent, thus we do not make such argument for this case.

Data covered by trade or professional secrecy must be exempt from any data sharing obligations. In line with diverse data processing abilities in public sector bodies, the lack of cost compensation or other incentives in situations of public emergency may hinder the timeliness and effectiveness of emergency response given potentially scarce time, resources, and financial means for the procurement of such data within organisations. In addition, potential support from businesses vis-à-vis public sector bodies when it comes to choosing, understanding, preparing, or even analysing the respective data may suffer.

From a privacy perspective, pseudonymising and anonymising data requires significant time and effort to achieve and merits adequate compensation in return. In addition, it is not fully consistent between parts of the text and the recitals, whether data has to be anonymised or pseudonymised, we suggest requiring pseudonymising instead of anonymising data.

Furthermore, companies should not be held liable for the data they share. We also suggest clarifying how legal review would interact with the 5 or 15 working day regime to vet incoming requests, respectively. In that context, clear definitions are furthermore highly important as it might be very difficult for companies to contest the public sector's request with the given time frames and potential fines (Art. 83 GDPR as referred to in Art. 33).

It appears problematic that the obtention of data to the potential detriment of a data holder could be based solely on significantly reducing the administrative burden for other enterprises (different from the data holder). Furthermore, who determines if and how the administrative burden has been reduced significantly? We suggest that such assessment should be performed by the data holder.

In addition, we would expect further details regarding the level of discretion public sector bodies have in setting a deadline that an enterprise has to comply with.

Chapter 6 – Switching Data Processing Services

In general terms, we welcome the idea to make switching easier for users of data processing services. At the same time, we understand that there are various points of view regarding the existence of lock-in effects on different cloud models (IaaS, PaaS, SaaS).

However, we underline the importance of

- Involving all market participants in such discussions
- Learn from and supplement existing self-regulatory efforts within the industry
- Acknowledging the complexity of such activities

- Providing additional guidance regarding technical implementation

We acknowledge the intention to foster and safeguard a maximum level of switching including data, applications, and any other digital asset for customers of a data processing service provider. The definitions of key terms, though, are often too wide or not given at all.

For instance, customers shall also be allowed – and the service provider must remove any obstacles for doing so – to port any "application" even if they merely have a right to use it and the "application" is an intrinsic part of the data processing service. Given the fact that the term "application" is nowhere defined, it can be construed to mean that a service provider has to assist a customer to port **its whole service offering** to the target service provider – which clearly cannot be meant. Against that background, we suggest to – as a first step - define more narrowly which exact architecture elements are within scope.

There is also a question as to whether the many categories of data to be made portable are all necessary for the switching process. The more data is exported, the longer the switching period will be.

More clarity is needed regarding the definition of "functional equivalence", and how it would be guaranteed. It seems the rules should only apply to removing obstacles under the outgoing provider's control.

Overall, we believe that these measures need to be nuanced and take into account the practical implications of the provision of cloud services.

Chapter 7 – International Data Transfers

It is yet unclear what would constitute an acceptable "legal, technical and contractual measure" and how each providers' tools would be assessed, keeping into account product developments over time.

By introducing safeguards against non-lawful access requests to non-personal data, legal certainty and trust in cloud infrastructures can be strengthened, which would benefit the overall uptake of cloud solutions in the industrial space.

Since providers of data processing services are required to verify potential requests from non-EU/EEA authorities, there need to be clear guidelines against which criteria such assessment needs to be undertaken. We welcome that the Commission included provisions in Art. 27 to provide additional guidance related to the verification process. To be effective, these guidelines should be developed on the basis of industry consultation. They also need to be made available before the Data Act becomes legally applicable.

More clarity is also needed regarding the requirement to take "all reasonable technical, legal and organizational measures" to prevent unlawful access or transfer of data

outside the EU. Recital 78 mentions a number of examples for such measures including the encryption of data, frequent submission to audits, verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies. The precise nature of the safeguards that need to be implemented should be better clarified however, e.g., via a cloud rulebook at EU level, and should take sufficient note of existing standards and frameworks developed by cross-sectorial initiatives such as Gaia-X.

Chapter 8 – Interoperability

Contrary to the narrow requirements for data processing services providers to allow and assist switching, the provisions regarding data spaces (Art. 28) solely remain an exercise in documentation unless the Commission issues further legislation concerning the essential requirements.

The current formulation also seems to focus somewhat narrowly on data spaces being operated by a single operator who would be obligated. Besides the fact that the term "operator" is not defined anywhere in the proposal, this does not provide a fair representation of the current set up of many data spaces which always consist of a governing entity which contracts out the actual operation of the data space ecosystem services to a suitable other entity. The proposal also fails to take into account federated (i.e., where more than one operator exists) or decentralized (i.e., where no set of operators can be identified) data spaces.

The terms "data space" and "operator" also need to be defined at all; neither the recitals provide guidance on the exact extent of this term (and, for instance, its delineation from a "data platform").

The idea to require an EU "declaration of conformity" for smart contracts is ambitious. No other type of software is required to provide such a declaration (notably including embedded systems for autonomous driving or AI/ML applications) and the existing laws of product safety and tort law seem to suffice.

Chapter 9 – Implementation & Enforcement

We believe there is a need to fully spell out the liability, remedy, and penalty regime instead of transferring such discussion to member state level in certain cases. This would avoid a potential gap along enforcement lines, discourage forum-shopping and prevent fragmenting the single market.

The Data Act entitles member states to establish new competent authorities for the enforcement of the Regulation but at the same time leaves the responsibilities to Data

Protection Authorities as far as personal data is concerned. A complex division of competences should not lead to diverging requirements (between member states) and/or legal uncertainties.

Chapter 10 – Database Directive

We believe that Art. 35 heavily restricts database protection and the associated investment incentives as the whole database (regardless what data not related to Art. 4 or 5 it contains) is left unprotected. Such far-reaching restriction seems neither necessary nor appropriate in order to achieve the declared goal of safeguarding the rights under Art. 4 and Art. 5. Rather than removing database protection entirely, the database protection right should be exhausted (only) where data access or use is permitted under the Data Act.

Additional clarification would be needed in regards to (i) whether the sui generis right is inapplicable only in the cases where it hinders the rights of users to access and use data under Art. 4 or the right to share data with third parties under Art. 5; (ii) what happens in the case of a database that has data obtained or generated by the use of a product or protected device, but in relation to which the owner has made a substantial investment in verifying or displaying the data.

Detailed comments on selected items

Recitals

Recital 6

"[...] In order to realise the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use."

- The claim that data is a non-rival good is problematic since data does not "just come into being", but always requires a prior investment decision; otherwise, such an understanding can have an innovation-inhibiting effect.
- It should also be added that competitive advantages can be gained around rival goods on the basis of data - e.g., in negotiation situations in which one negotiating partner has virtually disclosed all negotiating positions due to obligations of data transparency. Here, data could quickly have the significance of a trade secret without necessarily having the status of a trade secret formally.

Recital 14

"Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. [...]"

- Is it enough that devices are "able" to communicate data via a publicly available electronic communications service or do such devices have to be actually connected to such service?
- Almost all devices today already collect data. Even if a device is not yet "online", the mere application of a GPS tag onto it could do the trick. With this logic, one could turn virtually any "product" into a product within the meaning of the Data Act.

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. "

- Against that background, it is further unclear how smart phones per se are excluded but smartphones attached to a smart home seem included. In addition, would a smartphone with a downloaded app to command a smart home system be included in the scope?
- Printers should be added to this category since they are primarily designed to display content. Also, some printers have integrated scanners which are included. It should be ensured that the recitals, in particular recital 15 at hand, are taken into account for the product definition.

Recital 20

"...Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder. This means that data should only be made available when the user actually wants this. Where automated execution of the data access request is not possible, for instance, via a user account or accompanying mobile application provided with the product or service, the manufacturer should inform the user how the data may be accessed."

- One device could have multiple users. It is unclear how data access to the user would be (technically) implemented in practice (e.g., for a networked printer).

Recital 21

"Products may be designed to make certain data directly available from an on-device data storage or from a remote server to which the data are communicated. [...]"

- We would appreciate clarification that access directly to the IoT product and via a remote server constitute equivalent options is due to the heterogeneity of products that fall under the Data Act. Otherwise, necessary concepts (e.g., due to cyber security threats/prerequisites) cannot be deployed anymore.

Recital 23

"Before concluding a 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 how the data generated may be accessed"

- It is not clear if this can be achieved under the Terms and Conditions (T&C) or if this has to be clearly disclosed before the purchase or the product/service. Considering the reference to GDPR Art. 12-14, regulators might consider a separate disclosure would be needed. This would increase the cost of launching and maintaining a product in the market.

Recital 24

"This Regulation imposes the obligation on data holders to make data available in certain circumstances. Insofar as personal data are processed, the data holder should be a controller under Regulation (EU) 2016/679. Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation. However, this Regulation does not create a legal basis under Regulation (EU) 2016/679 for the data holder to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder. This Regulation should also not prevent sector-specific regulatory requirements under Union law, or national law compatible with Union law, which would exclude or limit the use of certain such data by the data holder on well-defined public policy grounds. "

- It should be clarified that the Data Act does not constitute a legal claim for users to request personal data of other data subjects. The current wording suggests that such claim exists, and it is upon the controller (data holder) to assess if there is an adequate legal basis under applicable data protection law to provide access to other

data subjects' personal data to the user. Such conflict between access rights based on the Data Act on the one hand and Art. 6 para 1 GDPR on the other hand puts a disproportionate burden on controllers. An access right to personal data of other data subjects would also possibly conflict with the objectives of the GDPR as set out in Art. 1 GDPR.

Recital 31

"Data generated by the use of a product or related service should only be made available to a third party at the request of the user. This Regulation accordingly complements the right provided under Article 20 of Regulation (EU) 2016/679. That Article provides for a right of data subjects to receive personal data concerning them in a structured, commonly used and machine-readable format, and to port those data to other controllers, where those data are processed on the basis of Article 6(1), point (a), or Article 9(2), point (a), or of a contract pursuant to Article 6(1), point (b). Data subjects also have the right to have the personal data transmitted directly from one controller to another, but only where technically feasible. Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner. The right under this Regulation complements the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in several ways. It grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data coming within its scope, whether personal or non-personal. It also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679, including the right to data portability, by seeking remedies in accordance with that Regulation. It is to be understood in this context that, in accordance with Regulation (EU) 2016/679, a contractual agreement does not allow for the processing of special categories of personal data by the data holder or the third party. "

- Art. 20 GDPR sets out certain requirements for the right to data portability. It is not clear why this regulation extends this right significantly.
- Recital 31 sets out that the data subject should be in no way prevented from exercising Art. 20 GDPR where the data holder and third party are unable to agree terms for direct access under the Data Act. In these cases, it should be clarified that the requirements for exercising the right to data portability as set out in Art. 20 GDPR remain unaffected by the provisions of the Data Act.
- Who is the user?
  - Example of a coffee vending machine in a company. Hypothetical scenario: a manufacturer produces a large coffee vending machine [manufacturer]. Company ABC CoffeeInvest acquires it [owner] and rents the vending machine to DEF CoffeeMakers [operator], who install the vending machine as a service at their customers' premises, e.g., GHI NewStartup GmbH [contractual partner], so that their employees [users ieS, > 100] have good coffee. DEF CoffeeMakers has contracted out the maintenance of the machines to JKL CoffeMaintenance & Co [maintenance company]. Who has what role here?
    - Manufacturer Interest: Telemetry data for product development, data owner if applicable.

- Owner: Interest in telemetry data for recording the use of the machine, possibly data owner, use for mapping the "leasing of coffee machines" business model
- Operator of the machine: Interest in telemetry data for recording the use of the machine, use for mapping the business model "Operation of coffee machines as a service", data owner, if applicable.
- Contractual partner for the service (company)? Telemetry data for recording the use of the machine, use for "provision of coffee for employees, suppliers & customers".
- Maintenance company? Telemetry data to optimize maintenance, use of the machine to "facilitate maintenance".
- Person who wants coffee: no benefit from the data. At the same time, no recording of individual users ("whoever wants coffee"). Implementation of data transfer? But users of the machine in the primary sense.

Recital 44

"To protect micro, small or medium-sized enterprises from excessive economic burdens which would make it commercially too difficult for them to develop and run innovative business models, the compensation for making data available to be paid by them should not exceed the direct cost of making the data available and be non-discriminatory."

- Larger companies should be able to receive compensation from small and medium-sized companies that exceeds the direct costs as long as such compensation is fair and reasonable. Then, larger companies can be incentivized to collect and share additional data with smaller companies, even if larger companies themselves do not directly benefit from this data.
- Does the profit margin depend on the size of the company? If yes, is there a table, depending on turnover / profitability / #staff, which defines the percentage margin depending on the size of the requesting company? Is it clearly defined how the "production costs" of the data are determined within a group?

Recital 45

"Direct costs for making data available are the costs necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production. Direct costs for making data available should be limited to the share attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will have to be set up permanently by the data holder."

- Can cost incurred to design the product according to "accessibility by design" principle be added proportionally to direct cost?
- Definition of "direct costs" is too narrow. Exemplary costs for sensors would not be covered which erodes the incentive for companies to install better sensors in order to generate more accurate data. Compensation must be adequate to create incentives and promote innovation.

Recital 51

"[...] Such contractual imbalances particularly harm micro, small and medium-sized enterprises without a meaningful ability to negotiate the conditions for access to data, who may have no other choice than to accept 'take-it-or-leave-it' contractual terms. [...]"

- Bargaining power is not a question of size of the contracting parties. Instead, it depends on the fact whether there is an alternative way or a competitor from which data or services can be received. Therefore, not only SMEs but also big companies can be subject of contractual imbalances.

Recital 64

"[...] The data holder should take reasonable efforts to anonymise the data or, where such anonymisation proves impossible, the data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available. "

- It would be of great practical use to have clear guidance on when personal data are anonymized/pseudonymized. In addition, the discussion in Germany about the necessity of a legal basis for anonymization is not supportive.
- Who bears the costs for this? These must be chargeable (direct provision costs), otherwise holding data becomes a burden.

Recital 77

. "In the absence of international agreements regulating such matters, transfer or access should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data. Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality."

- This will require a similar approach to Data Transfer Impact Assessments (DTIA) in the personal data space, but with considerable increased complexity (as we might need to perform legal analysis on IP and consumer protection law (amongst other areas)). DTIAs are proving to be one of the most complex topics in personal data management and this considerably expands their scope. Clear rules and limits on the requirements to conduct assessments by companies are needed. Verifying a third country legal system is not only overly burdensome but it would impose additional costs to companies operating in the EU which would impact their ability to compete globally.

Recital 78

"...In order to prevent unlawful access to non-personal data, providers of data processing services subject to this instrument, such as cloud and edge services, should take all reasonable measures to prevent access to the systems where non-personal data is stored, including, where relevant, through the encryption of data,the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies"

- This might be a bit too detailed opening for further secondary guidance to be issued on security, where other instruments such as GDPR are not as prescriptive. Instead, an approach similar to GDPR should be taken where companies should implement "appropriate technical and organizational measures" to protect data. Companies know the nature and risk of the data they hold and what would be the effective security measures. Mandating specific requirements would impose unnecessary burden on some companies.

Recital 79

"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."

"the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services"

- This could have an effect to curtail some service offerings and limit technical and business model innovation. Standards ensure industry driven inputs and technical knowledge, this process by the Commission seems to limit that.

Chapter 1

Ch. 1, Art. 1, pt. 1

"'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording"

- The definition of the term "data" is rather unspecific. Therefore, it shall be specified that:
  - only raw data is recorded,
  - only data that are actually used by the data holder for his own business transactions are affected,
  - volatile data should not be included in the definition (else there would be an obligation to commence storing data that has not been stored yet, which would have adverse effects for privacy) and
  - no (warranty and / or liability) claims arise due to the nature of the data (data "as is").
  - The definition of "data" could be augmented to define data as in Recital 14 and 17.

Ch. 1, Art. 2, pt. 2

"'product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data"

- Internet of Things (IoT) refers to movable items. Including immovable items would be too broad and could relate also to data services which would normally not be considered IoT. In addition, even certain movable parts that are only movable for maintenance could fall under the definition. Thus, we suggest deleting "including where incorporated in an immovable item".
- It should be ensured that the recitals, in particular recital 15, are taken into account for the product definition.

Ch. 1, Art. 2, pt. 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"

- Given the intended focus is on product manufacturers and their related services, we suggest narrowing the scope product functions (back) to core functions. Else, virtually any type of related service would be included from any actor.
- Data services that may use data of a product but are not directly connected or sold with the product should be out of scope. Thus, we suggest specifying:

  "'related service' means a digital service, including software, which is incorporated in ~~or inter-connected with~~ a product **and is part of its sale, rent or lease** in such a way that its absence would prevent the product from performing ~~one of~~ its **core** functions **as stipulated in (2)**;"

Ch. 1, Art. 2, pts. 2 and 3

- With respect to the definition of products and related services, further clarification is needed: data obtained, generated, or collected by the use of a product or related service that has so far not been transferred from the product or processed by a related service could suddenly fall under the obligations in chapter 2, such as device-only databases for the proper functioning of the product or data that is intentionally only stored on the product for security reasons (e.g., biometrics).
- First, this could have adverse privacy and security implications to the detriment of the end-user who is meant to profit from Art. 4 and 5 as certain data would suddenly have to be made available upon request.
- Second, how granular is a possible opt-in requirement?
- Third, given the current proposal, it is not clear whether such obligations would also apply to existing products and related services on the market or in use where such changes could be enormously costly or virtually impossible to implement in an economically feasible manner.
- Last, it could in principle force product manufacturers to become suppliers and/or competitors in an aftermarket that they have not yet participated in for various reasons with specific types of data. This seems to conflict heavily with entrepreneurial freedom to the detriment of product manufacturers.

Ch. 1, Art. 2, pt. 5

"'user' means a natural or legal person that owns, rents or leases a product or receives a service"

- According to Art. 3, a "user" is the owner, renter or lessee of the product or has purchased a service. He is therefore a contractual partner with regard to the product or service. This person bears the risks and, conversely, should enjoy the benefits of using the linked product and accordingly also have access to the data they have generated (Recital 18). The link via a corresponding contractual relationship is not expressed clearly enough by the wording "or receives services", but should rather go in the direction of "contracts services".
- For the building sector, for example, the user is not defined with sufficient precision. The contractual partner is the landlord, but at the same time, the tenant could also fall under the definition.

Ch. 1, Art. 2, pt. 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"

- The term is not sufficiently specified. Does it relate to a "person" who creates the product or a "person" who "controls the data"?
- The term suggests that there was only one data holder for each product. In practise, however, complement products may entail several data holders that each control separate parts/complements of the complement product. This can be analogue for services.
- For example, who should be the "data holder" regarding third-party apps that are offered in the product "vehicle" and that generate data? In the field of mobility services, **multiple players** are regularly involved (OEM, lessor, rental company, fleet operator, etc.). These actors have **different access possibilities** (technical and legal) to the data generated in the vehicle. In addition, the definition should be linked to the fact of **actual influence** on the data (data holder). It should be known from other online services that the manufacturer of the end device is not always the "data holder"; e.g., when using cookies.
- For further considerations and a concrete example, see our comments on Recital 31.

Ch. 1, Art. 2, pt. 10

"'public emergency' means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s)"

- We miss clarity and predictability regarding the scope of public emergencies. We suggest narrowing it down and specifying remaining cases more precisely and explicitly. In the German context, for example, state governments would have the ability to declare public emergencies, in that line, virtually any level of administration could hold such rights. Thus, we suggest adding:

  "[...]., which affects a significant share of the population."

  in order to create consistency

Ch. 1, Art. 2, pt. 17

'electronic ledger' means an electronic ledger within the meaning of Article 3, point (53), of Regulation (EU) No 910/2014

- This seems to be wrong. Art. 3 point 53 does not seem to exist. Nor a definition of electronic ledger is included in other articles.[10]

[10] https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

Chapter 2

Ch. 2, Art. 3, para 1

"Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user. "

- The scope of the data that must be shared is unclear. It lacks clarification whether all data generated during operation of a product must be made available or only data that is available for the data holder. Thus, we suggest:

  "[…] **that data generated by their use and reasonably available to the data holder are,** […]"

- From a technical perspective it is not feasible to realize the constant availability of all generated data from certain products. First the amount of the data itself will be tremendous for certain industries (e.g., automotive). Second the data itself is not available to the manufacturer (e.g., OEM). Third ecological costs would be immense as all the data would need to be stored at data centers that consume significant energy.
- Achieving this for some products would entail a significant redefinition of the data architecture. This can't be achieved in a short span as product development lifecycle is some time very long. If this article is enacted, it should contain a longer implementation timeline. In addition, the life cycle of the devices equipped with batteries would be considerably shortened.
- This requirement brings Privacy by design principles into non-personal data ("accessibility by design"). It should be specified that this does not create additional documentation burden for companies.

Ch 2, Art. 3, para 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: […]"

- Fulfillment of information obligations in cases where there is no direct relationship with the user (e.g., rental) is problematic. The Data Act does not specify who is obliged (manufacturer that collects data or company that holds the contract with the renter). The obligation should only be fulfilled within the chain of contractual relationships and may have to be passed on.
- Not clear if this is beyond T&Cs, but in any case, the information would need to be presented before acquiring the product or service. This might create some logistical problems in the case of purchases in retail. Additionally, this might require some modifications to the out of the box experience in some products. The product development lifecycle on some products is longer and therefore adequate time should be allowed for the implementation of this requirement if approved.

Ch 2, Art. 3, para 2, pt. b

"whether the data is likely to be generated continuously and in real-time"

- Real-time may mean immensely different time lags depending on the vertical and application at hand (microseconds vs. multiple hours).

Ch. 2, Art. 3, para 2, pts. d and e.

"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"

- Not clear how this will be dealt with on subscription models or how it may impact programs with channel and retails partners. The same applies to Ch. 2, Art. 3, para 2, pt. e. Sharing via such programs would have to be disclosed prior to purchase, disclosure will be complex for companies with a global reach.

Ch 2, Art. 4 and 5 (B2C and B2B data sharing)

- The relationship between Data Act and AI Act is not sufficiently clear. In particular, it is unclear if and, if yes, in what manner, data portability obligations in Art. 4 and 5 would interact with chapter 2 of the AI Act. In a nutshell, AI Act chapter 2 envisages certain transparency obligations in the context of data used in pre-trained models both during development and post-market settings vis-à-vis users. Who in the supply chain of pre-trained models has access to such data, do they have to and are the allowed to share it with users and/or third parties?
- The Data Act does not include a definition for "competitor's product", which is however of the utmost importance for the economy and the principle of fair competition. In this respect, the following two points, among others, should be addressed:
  - Does the term "competing products" only mean products as defined in this regulation and consequently only physical and movable objects? Or does the term "competing products" go beyond the definition and also includes related services, i.e., software and data-driven services? If so, is it intended that large software providers or service providers (outside the EU) could benefit indirectly by developing (software-driven) products/services based on the extracted data, which in turn compete directly with the original product/service? That cannot be the purpose of the Data Act.
  - It is necessary to define **delimitation criteria** in relation to sales markets (is a Chinese company a competitor for a European OEM?), timing of marketing (will a product launched in ten years based on today's data be regarded as a competing product?), special features under company law (is a newly founded subsidiary of an existing company a competitor?) etc.
- The general conditions of the contractual structure according to Art. 4 (6) for non-personal data are uncertain. What are the effects of terminating such a contract between data holder and user? The data, once given to the data holder, must remain with him.
- The obligations regarding the product design described in Art. 3 para 1 would require significant lead times for production and development within the automotive and supplier industry. In this respect, we see the planned implementation of the Data Act with only 2-3 years' time as not or only partially feasible for the automotive industry.

- There is need for clarification as to whether data that is also indirectly related to the use or purchase of the product should fall under the provisions of Art. 3 para 1. This applies in particular to industrial data that is only indirectly related to the product itself, such as data that reflects the degree of recyclability / reusability of a product.
- In addition, for a vehicle with an assumed service life of 15 years, it is impossible to predict the data usage that will occur over the course of said service life. Therefore, it seems rather impossible to sign an unchangeable contract with the user before any product purchase. It is also unclear what kind of corresponding information (and by whom?) should be provided in the event of a resale.

Ch. 2, Art. 4, para 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."

- The obligation to provide data in "real time" is practically impossible to implement. The concretization "where applicable" remains unclear. Basis should be data generated and available.
- This would require massive investment in data governance and/or process delivery as well as data architecture. Mandating real time access will create additional costs that will hinder the competitiveness of companies operating in the EU and may not be feasible for certain products. If this article is enacted, it should a longer implementation timeline should be provided.
- Also because of differing judicial practise in member states, we would welcome a clear definition of "undue delay".

Ch. 2, Art. 4, para 4

"The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate"

- In practice, delimitation difficulties can arise here. What if the user provides access to a third party that already offers a competing product? Can the third party use the data to optimize its own product?
- This prohibition needs to be extended to third parties where the user shares the data.
- In line with our comments above, we suggest extending this provision on related services. It is important to state that a prohibition to compete with the product or related service that the data originated from does in no way prevent a third party from offering an (aftermarket) service that may be in competition with a product or related service other than the one the data originated from.

Ch. 2, Art. 4, para 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."

- The necessity of a contractual agreement with the user is very problematic from an OEM-perspective as the OEM does not always conclude a contract directly with the user (e.g., leasing, rental car, etc.). Furthermore, data may also be required without consent for product monitoring and to enhance the security of the product. The restriction as formulated in the Data Act can have an innovation-inhibiting effect. It also limits the disclosure to cooperation partners for R&D and can thereby inhibit research and innovation.
- This seems to much restrict automatic data collection from device as it limits use of non-personal data to that specified in a contractual agreement. It will also impact the need to apply anonymization to all data. It limits the use of said data for "personalization" or tailoring of a product and service. Profiling is already covered under GDPR, but it extends this beyond personal data and could impact corporate customers for commercial services and products in the "industrial" BU thus hindering the ability to innovate in products and services.

Ch. 2, Art. 5, pt. 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"

- In the recitals, it mentioned this level of data access to the User (free, real time, etc.), but not to the third party where it did not specify continuous and real time and not necessarily free. Furthermore, the recitals address data associated with a service and seemed to discount data that was not associated with a service. This clause seems to potentially go wider than what the recitals state as the intent and turns solely on the user's demand. In addition, the implications for programs with channel partners are unclear.
- We would appreciate clarity to what extent a "request by a user who is the data subject" already constitutes valid consent under Art. 6 GDPR.

Ch. 2, Art. 5, para 5

"The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.."

- It is unclear how this would impact channel partners who want to develop their own service offerings or where they distribute from multiple OEMs. This would have economic impacts and therefore hinder investment in R&D.

Ch. 2, Art. 5, para 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."

- It should be clarified that the Data Act does not constitute a legal claim for users to request personal data of other data subjects. The current wording suggests that such claim exists, and it is upon the controller (data holder) to assess if there is an

adequate legal basis under applicable data protection law to provide access to other data subjects' personal data to the user. Such conflict between access rights based on the Data Act on the one hand and Art. 6 para 1 GDPR on the other hand puts a disproportionate burden on controllers. An access right to personal data of other data subjects would also possibly conflict with the objectives of the GDPR as set out in Art. 1 GDPR.

Ch. 2, Art. 5, para 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."

- This is a critical paragraph as – by matter of principle – trade secrets should by definition never be disclosed to a third party. The mere risk of having to disclose trade secrets could make companies not collect such data in the first place, with potentially far-reaching consequences for the future data economy.
- If this provision were to remain, enforcement of such agreement would be severely difficult and potentially put smaller actors at disadvantage.

Chapter 3

Ch. 3, Art. 8 (Conditions)

- Generally, the conditions in chapter 3 are not sufficiently precise.
- Data recipients are third parties, and this list of requirements is burdensome for the data holder. It may be appropriate to give the user control over the data in the out of the box experience or initial setup where the user can decide whether to consent to product data to be shared with the manufacturer or not, and whether to share with it a third party.

Ch. 3, Art. 8, para 3

"[...] 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."

- A reversal of the burden of proof to the detriment of the data holder appears open for abuse to the detriment of data holders who engage with a significant number of data recipients and may even put confidential business information at risk. In German civil procedural law, the principle of provision applies, i.e., each party must prove the facts on which their claim is based. Research evidence that runs counter to this principle is therefore fundamentally inadmissible. In this respect, the data access claims of the Data Act must not lead to a shift in this constitutionally recognized principle of court procedure (as in the case of a discovery under American procedural law).

Ch. 3, Art. 9, para 2

"Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs

directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly. "

- The scope of the companies defined as SMEs is too extensive.
- In any event, where micro, small or medium enterprise have a profit motive in processing the data received, it should be possible for the data holder to agree on a reasonable compensation with the data recipient.

Chapter 4

Ch. 4, Art. 13, para 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."

- Scope of enterprises defined as SMEs is too extensive and leads to an excessive restriction of freedom of contract.

Chapter 5

Chapter 5 (B2G Data Sharing based on exceptional need)

- These provisions are very broad and thus open for interpretation. To prevent abuses, the definitions need to be narrowed down and made more precise and explicit. In particular, there is a need for restriction, regarding both the parties and clear criteria for classifying use cases.
- Conditions and transparency for data provided to research institutions are too broad/unclear. In particular, data sharing and use should only be allowed for research directly linked to the public emergency in question. In other cases, sharing data for research purposes would go too far as (sensitive) business data is concerned.
- Furthermore, we would welcome liability provisions regarding the use of such data by researchers. We also would welcome provisions and safeguards against the re-transfer of such data between research organizations.

Ch. 5, Art. 15, pt. c (specific task in the public interest [...] explicitly provided by law)

- With the current phrasing, it is unclear whether any task – entirely unrelated to data processing in principle – could be found dependent on the obtention of data due to administrative discretion, that is not the data per se has to be found in the explicit legal mandate, but it merely has to support a *higher* legal mandate? This would come with significant danger of abuse, which should be avoided.
- From this phrasing it follows that the regulator may define further "public interest" and widen the duty to provide data. Which regulator can provide such law? Member States? The European Parliament and the Council?

Ch. 5, Art. 15, pt. c (1) (Inability to obtain data, first case)

- Inability to purchase data on the market at market rates raises several concerns. Assuming data is available at market rate, what if the public sector body chose not to obtain such data given the prices even though it was available at market rate?
- Thus, we suggest specifying concrete requirements for the inability to purchase such data at market rates. It is arguably difficult to agree on a market price for certain sets of data, as there may be cases where data is offered by only one participant.
- Generally, in exceptional need, timely legislative measures are exactly the way to go in order to obtain data that is needed, instead of a catch-all-clause if there is an unspecified urgency that is **not** a public emergency (as these cases are covered with pts. a and b).

Ch. 5, Art. 18, pt. c (2) (Administrative burden)

"obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises."

- It appears problematic that the obtention of data to the potential detriment of a data holder could be based solely on significantly reducing the administrative burden for other enterprises (different from the data holder). Thus, we suggest the following wording:

  "obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders ~~or other enterprises~~."

- Who determines if and how the administrative burden has been reduced significantly? We suggest that such assessment should be performed by the data holder.

Ch. 5, Art. 17, para 2, pt. e

"inform the data holder of the penalties that shall be imposed pursuant to Article 33 by a competent authority referred to in Article 31 in the event of noncompliance with the request"

- It is difficult for a data holder to contest the request due to high penalties that refer to the GDPR. Here, a provision that excludes the imposition of fines for actions during the initial request review period of 5 or 15 working days, respectively, could be helpful but potentially still insufficient to address this risk.

Ch. 5, Art. 19, para 1, pt. c

"destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data have been destroyed."

- As a data holder it is difficult to ensure that the public sector body (potentially in another member state) in fact complies with those requirements. Such compliance should be documented and monitored adequately.

Ch. 5, Art. 20, para 2

"Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin. [...]"

- The pseudonymization as required under Art. 18 para 5 may lead to costs as well.

- What exactly can be considered reasonable in that context?

Ch. 5, Art. 22, especially para 4

"After having been notified in accordance with paragraph 3, the relevant competent authority shall advise the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the relevant competent authority into account."

- Although the requesting public sector body from another Member State shall take the advice of the relevant competent authority, it may be challenging for a for example German company to fulfil the request of an Italian authority due to language or contextual differences. How can it be made sure that the request is adequate and complies with the requirements of Art. 17?

Chapters 6 and 8

We are still working on more precise comments regarding chapters 6 and 8 and intend to publish them as soon as possible.

Chapter 8

Ch. 8, Art. 30 (Essential requirements for smart contracts)

- General IT security and other established technical standards regarding development and deployment of software/applications (smart contracts are applications) already apply today, thus we doubt this article is necessary.

Ch. 8, Art. 30, para 2

"The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall perform a **conformity assessment** with a view to fulfilling the essential requirements under paragraph 1 and, on the fulfilment of the requirements, issue an **EU declaration of conformity**."

- Reviewing smart contracts and issuing an "EU conformity declaration" will cause additional administrative challenges and strongly hamper innovation, especially in the field of blockchain, distributed ledger technologies and any other initiatives related to smart contracts.

Chapter 10

Ch. 10, Art. 35 (Database directive *sui-generis* right)

- Art. 35 states that the sui generis database protection provided for in Art. 7 of Directive 96/9/EC should not apply to databases containing data obtained or generated through the use of a product or a service associated with it. Thus, the Data Act explicitly wants to prevent that users' access rights to data and their use according to Art. 4 or the right to pass on this data to third parties according to Art. 5 from being hindered by the owner of a database right.
- In our opinion, Art. 35 has the following consequence: As soon as a database contains data (also, besides other data) that was obtained or generated through the use of a product or a service connected with it, according to Art. 35, the database

protection no longer applies per se for the entire database. This is true regardless of the economic value of the data and the underlying investment in the creation of the database. Art. 35 massively restricts database protection and the associated investment incentives. Such a far-reaching restriction is neither necessary nor appropriate in order to achieve the declared goal of safeguarding the rights under Art. 4 and Art. 5. The balance between data access rights and investment incentives demanded in Recital 28 will most likely not be achieved in this way ("At the same time, it aims to avoid undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product.").

- In addition, it is unclear whether Art. 35 is still applicable if data, obtained or generated through the use of a product or a service associated with it, has been processed beforehand. Even though such data is no longer included in the database as raw data but has been prepared in advance with further investments (cf. "databases containing data obtained").
- The goal of safeguarding the rights under Art. 4 and Art. 5 can easily be achieved through a better regulatory approach. Rather than removing database protection entirely, the database protection right should be exhausted (only) where data access or use is permitted under the Data Act. Such an exhaustion rule would also have the desirable consequence that in case of a violation of the usage restrictions in the Data Act (e.g., Art. 6 Para. 2), the owner of a database right - if all other prerequisites are fulfilled – could still enforce its database right against the non-permitted use under the Data Act.

  Thus, we suggest the following amendment:

  > "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/ ~~does not apply to databases containing data obtained from or generated by the use of a product or related service~~ **shall not entitle the data holder or proprietor of a sui generis right to prohibit the access and use of data that is permitted under this regulation**."

Chapter 11

Ch. 11, Art. 42 (Begin of application)

- Any type of regulation that imposes requirements on the design of products (e.g., the requirement to design systems to allow easy access to data) must provide adequate notice periods to adapt to the regulatory requirements. This is especially applicable to products with long development cycles (e.g., automotive). Attention must therefore be paid to appropriate transition periods, which are not yet identifiable in the draft.