bitkom

Bitkom Position Paper EU Data Act Proposal

April 19, 2022

Short 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 and comment on individual chapters 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

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[2] under negotiation, announced or proposed sectoral initiatives concerning data sharing, the GDPR, the existing e-Privacy Directive[3], the upcoming e-Privacy Regulation[4], the upcoming Digital Markets Act[5] 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.

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:[6]

- 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.

[2] COM/2021/206 final
[3] Directive 2002/58/EC
[4] COM/2017/10 final
[5] COM/2020/842 final
[6] https://www.bitkom.org/sites/default/files/2021-03/20210315_-bitkom-principles-digital-markets-act.pdf

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.

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.

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

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 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.

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.[7] 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.

We struggle to identify an addressable market failure for the cases related to public emergencies (Art. 15 pts. a, b)[8] 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

[7] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954
[8] Art. 15 pt. c 1 includes a market failure test to some extent, thus we do not make such argument for this case.

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.

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.