VERBAND DER INTERNETWIRTSCHAFT E.V.

Position Paper on the European Commission's proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (COM (2022) 68 final)

Berlin, 13.05.2022

On 23 Feb. 2022, the European Commission presented its draft Data Act. With this draft, the Commission is pursuing the goal of making better use of data. From the perspective of the EU Commission, this would not yet be done to a sufficient extent to harness the full value-creation potential of data for the European economy. In addition, the Commission implies that much of the data is owned by a few players. The Data Act is intended to create legal certainty regarding the sharing and use of data and also establish new rights and obligations for data holders to open up their data assets to their users or other third parties. The Data Act focuses to a large extent on non-personal data, such as that generated by connected products like cars, smart wearables or smart home devices. Alongside the Data Governance Act (DGA), this is one of the EU Commission's central projects in the area of data policy in this legislative period and is part of the EU data strategy. Like the DGA, the Data Act is intended to support data-driven innovation and business models and make the European Union a leading location for data-driven services.

In the following, eco presents its initial comments on the present draft regulation.

I. General remarks

- **Data access and use**

The European Commission's goal is to make it easier to share and use data. In general, we welcome the Commission's intention to increase data access and use, based on the principle that the individual user should be at the centre when it comes to determining who has access to that individual data and for what purpose. However, the Data Act creates additional obligations for data holders, particularly with respect to sharing and accessing user generated data. In eco's opinion, certain requirements established in the data act, run the risk of thwarting the goal of the Commission. The focus of the Data Act should, therefore, be on creating incentives to make the sharing and opening of data assets to third parties more attractive to data holders.

General data sharing requirement on the other hand could jeopardize availability of data, if it is not checked against other objectives and principles of data procurement, as well as legal uncertainty in terms of GDPR and personal data that would be caught by data portability requirements.

Moreover, the Act does not sufficiently address issues relating to security and trade secrets that are raised by the access and switching requirements. While we agree that the objectives of the Data Act are important, they should be balanced by equally important standards to maintain the integrity of both security and trade secret information. We recommend inserting appropriate limitations to ensure that these rights do not result in access to data by nefarious actors that seek to exploit security vulnerabilities or misuse confidential commercial information.

- **Relationship to the GDPR**

The Data Act focuses to a large extent on on non-personal data from connected products and creates a right of access for users similar to the right afforded to data subjects under GDPR. Nevertheless, in many instances, the present draft relies on the GDPR, which provides the legal framework for the handling of personal data. In eco's view, the difference between personal and non-personal data should also be reflected in regulatory terms. This does not require a GDPR for industrial data, whereby the Data Act, in contrast to the GDPR, does not provide for the possibility of processing data for a "legitimate interest". Instead, it should always require a data license from the user.

II. The Data Act in detail

On Article 1: Subject matter and scope
Article 1(1) states on the scope that data holders must make their data files, including generated data, accessible "to their users as well as to "public bodies or Union institutions, agencies or bodies when there is an exceptional need for the performance of a task carried out in the public interest". eco considers this to be problematic, as the data generated by data-driven business models may contain trade secrets or allow conclusions to be drawn about them. The use of such data by the public administration requires a clear definition of the data in scope and when an "exceptional need" exists. Clear rules are also needed for compensation in such cases. Article 1 (3) refers to the previous rules on the protection of personal data, in particular the General Data Protection Regulation (GDPR). These continue to apply, unaffected by the Data Act. This requires additional differentiation and

potentially offers potential for conflict for companies in determining which category the data falls into in each case.

On Article 2: Definitions

Article 2 (1) adopts a very broad definition of data. For example, video and audio recordings are also included. Since products such as smart speakers are also covered by the Data Act, this definition could damage trust in connected products, especially since video and audio recordings are perceived as particularly sensitive by consumers. In light of the broad definition of “virtual assistants” in Article 2(4), it is unclear how data-sharing would impact liability of the parties involved. Software like virtual assistants don’t know how the software works on third party devices and how users are engaging with the hardware. Hardware manufacturers on the other hand have the ability to govern how their devices are being used and have contracts in place with software providers that also govern data generated by the interaction (on top of the data generated by the device which the device manufacturer collects). eco is also critical of the definition of “public sector bodies” in Article 2 (9). It affects all public entities, not just those directly or indirectly affected by emergencies, such as those for public safety. In light of the broad rights granted to “public bodies” under the Data Act, a more narrow and more precise definition would be desirable. “Exceptional need” is not defined under Chapter I, but is a key concept under Chapter V, in particular if data holders are required to shoulder administrative burden in order to reduce the same for other enterprises. Thus, eco considers it is essential to make a clear distinction between the definitions of “public emergency” and “exceptional need”. Similarly, “good commercial practice in data access and use” and “fair dealing” are not defined under Chapter I, but are key concepts under Chapter IV. The definition of “processing” in Article 2 (11) is too broad in the opinion of the eco. Accordingly, simply storing the data is to be considered processing, and providers of such services thus fall within the scope of the Data Act. This means that housing and certain data hosting services are affected by the Data Act, even though the analysis of data is explicitly not part of their business model. Article 2 (12) defines “data processing services”. eco considers this definition to be problematic, as it overlaps with various other definitions of other, equally relevant legal acts such as the Digital Services Act, but also the NIS Directive, thus introducing more complexity into the overall regulatory structure.

On Article 3: Obligation to make data generated by the use of products or related services accessible

According to the wording of Article 3 (1), “Products shall be designed and manufactured, and related services provided, in such a manner that the data generated by their use are, by default, easily, securely, and, where relevant

and appropriate, directly accessible to the user." The Data Act directly applies to the product design and business models of manufacturers and providers of related services. The criteria raised in the text of the regulation are abstract and require further concretisation in order to be provided by manufacturers and service providers in a legally secure manner. This is not conducive to an innovative digital economy. Therefore, eco suggests to provide more clarity on appropriate transition arrangements in order to meet this obligation for product manufacturers. In addition, Article 3 (2) creates further information requirements (possibly in addition to the GDPR) that create barriers to use and bureaucratic burdens for companies.

On Article 4: The right of users to access and use data generated by products or related service

eco takes a critical view of the obligation of data holders to provide data in real time, which is enshrined in Article 4 (1). This is associated with a high level of effort and further costs for companies, which makes the generation of high-quality data less attractive and thus runs counter to the goal of the Data Act. Article 4 (3) provides that trade secrets shall only be disclosed to users if measures are agreed upon to maintain the confidentiality of the shared data, in particular with respect to third parties. In practice, however, this is likely to be difficult to track and verify and would place the burden of proof on the initial data holder which may impractical. Therefore, disclosure of trade secrets by invoking Article 4 (3) should be excluded.

On Article 5: Right to share data with third parties

According to Article 5 (1), data holders must make their data available to third parties, free of charge to the user, given a request of a user. According to Article 5 (8), this also applies to trade secrets in some cases. For this purpose, the data holder should agree on measures with the third party, which will ensure the confidentiality of the data. In the opinion of eco, however, implementation is problematic, especially since it involves an enormous amount of additional work for companies. This is especially true for high-volume transactions.

On Article 6: Obligations of third parties receiving data at the request of the user

Article 6 addresses the obligations of third parties in the handling of the data holder's data. According to Article 6 (1), the third party must delete the data received as soon as it is no longer required for the fulfilment of the commissioned service. Although this is understandable for reasons of data security and data minimisation, it does involve additional work for the companies. In addition, the purposes of the provision are not always traceable, as they are mandated by the user. This entails legal uncertainty

for the third parties. eco, therefore, views this critically. According to Article 6 (2c), the data can be shared with other third parties if this is necessary to provide the service offered. The possible involvement of other parties makes it more difficult for the data holder to enforce the confidentiality agreement, especially with regard to the disclosure of trade secrets. According to Article 6 (2e), the received data may not be used by the third party to develop a competing product. In the opinion of eco, a clear definition is required here as to when it is a competing product and not a further development or something similar. Moreover, 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 devices, but also to related services and virtual assistants. Otherwise, investments into related services and virtual assistants could be undermined. It is important to note that a prohibition to compete with the product or service that the data originated from does in no way prevent a third party from offering an competing aftermarket service.

On Article 7: Scope of business to consumer and business to business data sharing obligations

The exemptions for small and micro enterprises provided for in Article 7 are supported by eco. It is important – and consistent with the intent of the Data Act – that small businesses with innovative, data-driven business models be able to grow without being subject to excessive red tape.

On Article 8: Conditions under which data holders make data available to data recipients

The negotiation process described in Article 8 (2) between the data holder and the third party, regarding the conditions for data transfer, still requires some clarification and specification in the opinion of eco. It is unclear how such a process, especially for digital business models that tend to rely on standardised contracts, can work without creating a lot of extra work for companies. The prohibition of discrimination between data recipients set forth in Article 8 (3) is fundamentally understandable. However, the burden of proving that data is provided in a non-discriminatory manner rests solely with the data holder. The exception provided for trade secrets in Article 8 (6) is to be welcomed, but here too the burden of proof lies with the data holder. However, this too is likely to be difficult to prove in many cases.

On Article 9: Compensation for making data available

Article 9 (2) is intended to limit the amount of compensation that a data holder may claim to the cost of provision if the data recipient is an SME. In principle, this approach is appropriate for making data easier to use for SMEs. However, in practice, it is unlikely to encourage investment in data processing as a whole or the development of new services. Cost capping

also results in a reversal of the burden of proof since Article 9 (4) requires the data holder to prove that the costs of provision were not exceeded by the compensation and also to provide a precise breakdown of these costs. This creates additional bureaucracy that could make data processing less attractive overall. At a minimum such restriction should be limited to small and micro-sized companies. Extending it to medium-sized enterprises, as the Commission proposes, would represent a disproportionate intervention into the freedom of contract, by effectively setting a price-regulation for the vast majority of the market. Finally, it is also important to note that there is a potentially ambiguous interaction with the GDPR at this point regarding the possibility for data holders to claim compensation for data portability from data recipients under Article 20 of the GDPR.

On Article 10: Dispute settlement
eco welcomes the dispute settlement body named in Article 10 (1) in principle. It is positive that legal recourse nevertheless remains open to the disputing parties (Article 10 (9)) and that, in addition, the parties must agree on the binding nature of the judgment prior to the proceedings by the dispute settlement body, as stipulated in Article 10 (8).

On Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data
eco see positively the technical protection measures mentioned in Article 11 (1). However, a precise definition of what constitutes a “appropriate protection measure” is needed to provide legal certainty. The prohibition of obtaining data unfairly, for example by providing false information to the data holder or by using technical loopholes, as described in Article 11 (2), makes sense. According to eco, this prohibition is important to create trust in the data sharing process and the security of data.

On Article 13: Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise
Article 13 defines unfair contractual terms for the use of or access to data, which are to be ineffective vis-à-vis SMEs if they were imposed "unilaterally" on a contracting party, i.e. could not be influenced by a contracting party through negotiations. This results in the right of both contracting parties to be able to negotiate on any article. This seems impractical, especially in mass business, and would make data sharing unattractive because of the effort involved. While it is understandable that the Commission is trying to support SMEs, also in line with the goal of creating an innovative data economy in Europe, eco nevertheless rejects the far-reaching encroachments on contractual freedom associated with the proposed regulation. Moreover, the data holder bears the burden of proof that its terms are non-discriminatory

and that they were not unilaterally imposed. This creates a presumption that is extremely difficult to overturn. It should therefore be for the complainant to prove that the terms are discriminatory, as they will be the party holding the best evidence.

On Article 14: Obligation to make data available based on exceptional need

The purpose of Article 14 is to create an obligation for data holders to make their data available to the public administration in case of an emergency. Only small and micro enterprises are exempt from this obligation. This exception is supported by eco. However, eco would like to point out that an obligation to disclose data to public bodies, which are defined very broadly under Article 2, should only take place in individual cases and in extreme emergencies following strict principles of proportionality, purpose limitation and limited retention. A corresponding clarification would be desirable here.

On Article 15: Exceptional need to use data

eco welcomes the intention to harmonize the legal framework on B2G data sharing but the current text could lead to unintended consequences.
The definition of an “exceptional need” as made in Article 15 (1) is, in the opinion of eco, too broad and should therefore be revised. This is because the definition chosen covers not only public policy emergencies but also, according to Article 15 (1c), situations in which the “lack of available data prevents the public sector body or the Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law”. This broad definition could increase the number of requests for access to data and would impose additional burdens on companies as these are also relatively light justifications. The lack of precise safeguards afforded by the public administration for the data accessed especially regarding privacy, security and protections of business secrets and Intellectual Properties would create significant risks for data protection and make holding and processing data less attractive. In addition, there could be an unequal bargaining position between companies and public bodies, with public bodies being able to refer to the obligation to hand over data when negotiating the sharing of data.

On Article 16: Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies

According to Article 16 (2), “The rights from this Chapter shall not be exercised by public sector bodies and Union institutions, agencies and bodies in order to carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences (...)”. eco

welcomes the fact that the obligations of companies to disclose data to public sector bodies, as mentioned in Article 14, do not apply to law enforcement.

On Article 18: Compliance with requests for data
Article 18 (2) provides, in the case of requests by public sector bodies under Article 14 (1), a maximum period of 15 days to process them and react. However, rigid deadlines for verifying requestsmay be difficult to meet in some cases. eco, therefore, advocates a more flexible arrangement that allows companies a reasonable opportunity to respond and react to the requests and to discuss with the requesting authority any resources that may be needed.

On Article 20: Compensation in cases of exceptional need
Article 20 establishes a different level of compensation for the “exceptional needs” referred to in Article 15. Accordingly, in emergency cases, according to Article 15 (a), there shall be no compensation. In all other cases, the compensation shall be the provisioning costs plus a “reasonable margin”. In the opinion of eco, this differentiation and distinction are not appropriate. In addition, the compensation should also be allowed in cases where data is needed to respond to a public emergency, and it should be possible to exceed the pure provisioning costs in order to create real compensation for the additional obligations of the companies.

On Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs
According to Article 21 (1), public sector bodies and institutions may share the data they have received under Article 14 with non-profit organisations for research purposes, for analysis or for the production of statistics. eco argues that the decision on disclosure should be made by the data holder. Involving other parties also calls into question the confidentiality of trade secrets. There is also a need for a clear definition of who falls within the definition of a research organisation under Article 21. Competition-related issues may arise from the unclear definition. For example, a company’s think tanks could use this method to obtain data and information from a competitor.

On Article 23: Removing obstacles to effective switching between providers of data processing services
Article 23 and other articles are intended to create a new regulatory environment for data processing service providers. As more and more consumers, governments, and companies depend on cloud services, it becomes all the more vital to create a more open and dynamic cloud market. By enhancing the ‘switchability’ of cloud services, the Data Act can contribute to increase flexibility and choice for customers.

According to Article 23 (1), customers should be able to terminate a contract and switch providers at any time within 30 days. eco is concerned that the short notice period would hinder planning security for companies. Switching is a technically complex process that will generally involve more than just cloud providers. The complexity of this process should be taken into account, when defining a deadline. Moreover, it is also unclear what is meant with “functional equivalence” and how that would be provided, including which provider carries the responsibility to ensure it. Because of the great diversity of cloud computing services, eco advises that the measures in Article 23 need to include more nuance and take into account the reality of the provision of cloud services as well as complexity of switching project and potential need for technical assistance.

On Article 25: Gradual withdrawal of switching charges
Article 25 (1) provides for the prohibition of fees that data processing service providers may charge their customers after three years from the effective date of the Data Act. During the transitional phase, according to Article 25 (2) and Article 25 (3), it should only be possible to charge fees that do not exceed the costs incurred by the provider as a result of the switch. While eco understands the aim of the Commission to create an environment, which makes switching services and software easier for users, a complete removal of switching charges may in fact prove counterproductive for the uptake and running respective services for data holders. eco would agree to moderate and appropriate switching charges based on the administrative burden of the company transferring data allowing for a swift and efficient transition.

On Article 26: Technical aspects of switching
Article 26 (2) obliges providers of data processing services to use open standards and provide open interfaces. While inconclusive about the obligation, eco welcomes the approach of the Commission to foster and support open standards for data exchange.

On Article 27: International access and transfer
The obligations created by Article 27 (1) significantly complicate access to non-personal data by third country authorities, where such an access request is not covered by an international treaty and would be in conflict with Union or national law. The draft stipulates: “Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State (...).” Thus, the Data Act creates a regime that

is similar to the GDPR. However, while GDPR transfer limitations are motivated by the risks related to protection of fundamental rights, it not clear what is the rationale behind the limitation of non-personal data transfers. It is important to more precisely elaborate on what kind of third country laws needs to be assessed for conflict with Union law. In addition, the requirement to provide adequate measures to prevent unlawful access to non-personal data would also be subject to interpretation from various competent regulators leading to legal uncertainty. In eco's opinion, sectoral approaches are needed here that enable a more specific assessment to be made. The overlap between the Data Act and GDPR should be further assessed to ensure that the requirements related to the transfer of non-personal data would neither raise illegal trade barriers nor increase compliance burden and create unecessary red tape for companies

On Article 28: Essential requirements regarding interoperability
Article 28 is intended to promote the creation and establishment of common standards in the EU. To this end, Article 28 (2) empowers the European Commission to adopt legal acts to enforce these standards and Article 28 (4) to mandate European organisations to develop new standards. The standardisation of data formats is viewed positively by eco and is associated with the expectation that it will lead to greater and simpler use of data. However, the EU Commission does not need to be authorised to issue a regulation for this purpose.

On Article 29: Interoperability for data processing services
Article 29 refers to the creation of standards for data processing services. Accordingly, services of the same type should be interoperable. eco welcomes the creation of consistent standards in principle but points out the unclear definition of "service type". This is critical, as "data processing service" is defined very broadly in Article 2. In practice, this could lead to interoperability requirements for services that are not similar. As a result, this could lead to less innovation and choice for users, as services would have to converge.

On Article 30: Essential requirements regarding smart contracts for data sharing
Article 30 (2) states: "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". This obligation to carry out conformity assessments could generate additional effort and

costs. eco, therefore, suggests examining the extent to which a more proportionate design of the provision is possible here.

On Article 31: Competent authorities
Article 31 (1) provides that Member States shall each designate one or more authorities to be entrusted with the enforcement of the Data Act. In the opinion of eco, it would be desirable to create clear responsibilities. The limitation and definition of a competent authority would be expedient here in order to create clear responsibilities. This authority is also to be authorised under Article 31 (3d) to impose penalties retroactively. eco considers this possibility to be questionable and therefore rejects it.

On Article 33: Penalties
The amount of possible penalties for violations is specified in Article 33. In this regard, the Data Act makes use of Article 83 of Regulation (EU) 2016/679 (GDPR) for violations of the provisions from Chapters II, III and V. Accordingly, fines of up to €20 million or 4% of global sales are possible in the event of violations. In addition, penalties under Article 66 of Regulation (EU) 2018/1725 are also possible for breaches of the provisions in Chapter V, should the breaches have been committed by Union institutions. Fines of up to €500,000 are possible here. eco considers the proposed amount and assessment of fines of up to €20 million or 4% of annual sales to be too high. Particularly in light of the fact that the present draft may lead to cumulation with other fines, e.g., in the case of data protection violations, if, for example, personal data are affected. Furthermore, eco also considers the alignment of the fines with the GDPR to be disproportionate. Data without a personal reference is less sensitive than data with a personal reference. This should also be taken into account when determining and assessing the fine.

On Article 34: Model contractual terms
In Article 34, the EU Commission is to be empowered to create model contractual terms for data use and data access. From eco's point of view, these can be helpful, but they must be less bureaucratic and clearly formulated in order to create legal certainty and offer added value.

III. Conclusion

With the Data Act, the Commission seeks to increase data use and enable new innovative business models. In the area of the data-driven economy, Europe lags behind other regions of the world. eco therefore supports and endorses the EU Commission's initiative in principle. However, the current draft creates many new obligations and thus bureaucracy and costs for companies, which do not always make the collection and processing of data within the EU more attractive.

In addition, the obligation under Articles 3 and 4 interferes with product design. This has a negative impact on the development of new business models and innovative products. This thwarts the Commission's goal. The requirement to share data with third parties may also put trade secrets at risk because the Data Act's draft safeguards are inadequate. The same applies to the duty to disclose to public authorities set forth in Articles 14 and 15. An obligation to surrender should only be possible in exceptional cases and, moreover, only in legally standardised and clearly defined emergencies.

It is positive that the special concerns of SMEs have been addressed and taken into account in the present draft. The exemption of small and medium-sized enterprises from some obligations is appropriate. In eco's view, it is also necessary to distinguish the Data Act more clearly from the GDPR. This would create a more attractive environment for providers of data-driven products and services. The difference between sensitive and less sensitive data needs to be given greater regulatory consideration to further facilitate the use of data.

Furthermore, additional incentives should be created for companies to make data available. These incentives can also be economic in nature, to make generating and sharing high-quality data, in particular, more attractive. In this way, the importance that the generation and provision of data has for society would also be adequately taken into account. The envisaged creation of common standards and formats for data can also support higher data usage and thus contribute to the Commission's objective.

About eco: With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically-oriented digitalisation. That is why eco advocates for a free, technology-neutral, and high-performance Internet.