Warsaw, 14th July 2022

Directorate-General for Communications
Networks, Content and Technology
European Commission
1049 Bruxelles/Brussel
Belgium

To Whom Tt May Concern,

On behalf of the Digital Poland Association (Związek Cyfrowa Polska), the industry organization of employers, which brings together the largest companies from the RTV and IT industry operating in Poland, including manufacturers and importers and distributors of electrical and electronic equipment, I present our position to the proposed regulation entitled Data Act.

The following document sets out high-level points on issues of concern arising from the leaked draft of the European Commission's proposal for a Data Act ("proposal").

1. **Scope:** The scope as defined in the articles of the proposal remains unclear and arbitrary given it is to cover e.g. smart TVs and voice assistants while excluding desktop computers or smart phones which tend to fulfil in many case similar functions and can access the same services. The definition of 'data' itself is very broad and the question arises whether this covers only raw data or potentially business sensitive processed data. Further, the definition may equally cover security relevant data. The definition of 'related services' is also unclear as it fails to address the delineation of responsibilities between the stakeholders of the supply chain that are best positioned to give access to data.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

2. **Trade secret protection:** The proposal provides for disclosure of trade secrets to users, third parties and public bodies under conditions to preserve the confidentiality of the trade secret. However, it does not indicate how the legitimate interests of data holders would be protected in the event of unlawful use by third parties.

3. **Gatekeeper contagion**: The proposal carries forward the gatekeeper concept from the Digital Markets Act (DMA). A company designated as a gatekeeper under the DMA, would not be not eligible to receive any user data from consenting users and other services and may not incentivize customers to transfer their data to them. These limitations apply to the entire company irrespective even of whether this concerns its core platform service and would unreasonably place these companies at a competitive disadvantage. This is specifically concerning as the scope of the DMA, in terms of services covered, barely overlaps with the Data Act's scope. In consequence the use of the 'gatekeeper' concept in the Data Act appears somewhat arbitrary. Finally, this exclusion affects European users' rights to move their co-generated data to a service of their choosing, which constitutes a disproportionate regulatory intervention.

4. **Obligations of data receiving third parties:** Data receiving entities may not use the data to develop competing products but may develop competing services. The distinction of product and service makes increasingly less sense as manufacturers regularly monetize products via the service element. Allowing for the data of the source service to be used to develop competing services risks stifling R&D and investment. Furthermore, it is unclear how the non-compete provision would be enforced in practice the recipient would not necessarily be aware of competing products of the data holder. Similarly, the data holder would likely have no insights into any abuse of the data for competing products. Overall, once data is shared with a third party, it is not clear how the data holder would be able to control how the data is used, or what parties may access it further.

5. **International access and transfer:** The proposal mandates technical, legal and organizational measures to prevent international access or transfer of non-personal data held in the EU where such transfer or access would contradict EU laws or national law of the relevant Member State. Third-country requests for access or data transfer will only be

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

considered valid if based on an international agreement between the requesting country and the EU or EU Member State. The proposed procedural requirements would lead to *de facto* data localization requirements and discriminate cloud service providers legally established in Europe that may be subject to laws in another jurisdiction that could conflict with EU law, but without legal review. This could affect numerous major data flows without even a prior judicial assessment and restrict the choice of technology and the EU's capacity for innovation while limiting the ability for EU businesses, beyond digital platforms, to grow and compete internationally.

6. **Conditions for making data available to recipients:** The proposal places an unreasonable burden for a data holder to prove that the conditions for making data available are non-discriminatory, whenever an enterprise "considers" the conditions to be discriminatory. It is unclear why data recipients are accorded the right to make blanket allegations without substantiating their arguments.

7. **Making data available to public bodies:** While the proposal enables public bodies to acquire data where there is an "exceptional need", it does not include any safeguards for data holders that avail data to public bodies that then either use the data to harm the data holder. Euqally open is the question whether data of third parties or that allows conslusions about third parties is covered by government data requests.

8. **Cloud switching:** While the proposal has the legitimate ambition to facilitate switching between cloud providers, the cloud switching obligations do not reflect technical realities and risk negatively impacting EU customers' experience and choice of services. Cloud customers can determine the cloud services they want to use, how they architecture solutions based on the services they select, access, download and delete their data, and determine the appropriate format and storage location. CSPs create value for businesses by developing custom offerings to realize unique business solutions. Portability of workloads is a shared responsibility between CSPs and customers. The switching obligations should reflect the variation of complexities and choices involved in the switching process.

   Cloud service providers will be obliged to ensure customers retain 'functional equivalence' for similar services and ensure compatibility with open interoperability requirements when switching to another provider. This will inevitably lead to a race-to-the-

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

bottom and force CSPs to not innovate in ways that would benefit customers (QoS, security), risking homogenized services and removing benefits from combining multiple services within a cloud ecosystem. Customers should ultimately have the freedom to choose a solution that best meets their needs. CSPs should not be held responsible for the functional equivalence with a competitor's offering. CSPs should provide transparency about the service types they offer and how these would adhere to customer expectations on the ability to switch and port data.

CSPs should support the migration in and out from its cloud environment by providing customers with tools and information about these tools and for what services they apply. The timelines for switching should be agreed between the CSP and customer and the CSP should be allowed to recoup its costs incurred in the switching process (e.g. network usage). In addition, a CSP should not bear costs they have no control over such as costs for third part assistance in the switching process or third-party telecommunication costs for data transfer.

The switching obligations appear to overlap with the portability obligations under DMA, which urges to putting on hold the implementation of the DMA until obligations applicable to cloud computing providers are clarified under the Data Act.

9. **Interoperability:** The proposal empowers the Commission to adopt standards for which compliance with the Data Act provisions on interoperability is presumed. This is significant because the Commission's new Standardization Strategy appears and its review of EU Regulation 1025/2012 aim at reducing the cooperation of EU standardization bodies with international standardization bodies, thus decreasing the influence of non-EU companies in EU standard setting processes. This is worrisome as is unclear how the EU could avoid circumstances where standards are designed to disadvantage non-EU companies, both generally and with respect to compliance with the Data Act.

10. **Enforcement**: It is unclear why the enforcement of the Data Act, including levying of fines for non-compliance is split between different regulators and left to individual Member States. A decentralized system that affords Member States the discretion to enforce the rules would lead to different practices across the EU. It is not clear how that comports with the objective of creating a harmonized legal framework using Article 114 of the TFEU.

11. **Dispute settlement**: Data holders and recipient are entitled to use dispute settlement mechanism established in the proposal. However, this does not affect the right of the parties to seek an effective remedy before a national court or a tribunal. It is unclear how this would work in practice as it exposes companies to the risk of having one dispute before multiple fora.

In addition to the general comments set out above, we would like to make comments on the specific provisions of the proposed act.

B2B, B2C data sharing (chapter 2 & 3)

- The current definition of 'data' is too broad and may cause legal concerns especially in respect to GDPR. Thus, a clear definition of its content and boundaries, having in mind non-personal data, is needed.
- More robust trade secrets safeguards should be included to avoid undermining investments in innovation. This is particularly important given the broad definition of "data". Trade secrets protections should not differ depending on whether a user (which could be a business) or a third party is at the receiving end, or whether trade secrets relate **to a product or a related service**. Robust trade secrets protection should also be provided where a government shares with third parties any data it acquires from a service provider. References to the Trade Secrets Directive should be included throughout and severe consequences (not just judicial recourse) should be provided for any data recipients in the event of unauthorised disclosure of trade secrets.
- It is disputable whether the Data Act proposal is in line with the DMA (a point the impact assessment also makes). The Data Act seeks to address perceived barriers to data-sharing by applying to a wider range of services of alleged "gatekeepers". If the DMA designates a data holder as a gatekeeper, then there are regulatory obligations that kick in and competition law is still available to impose behavioural remedies to the extent the gatekeeper is found to be dominant and to abuse its market position. We would also flag that, excluding not just the data holder, but the entire undertaking to which the data holder belongs, from the possibility of being a data recipient is not necessary and excessive, especially when these are providers with a proven track

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

record of developing products and services that consumers value and that benefit SMEs. We would also point out that users may be more willing to try new products and related services by porting the data to new entrants in the space, if they are aware they have the possibility to go back to the original service provider in case they are not satisfied with the new products and related services used.

- Data Act sharing requirements go beyond the GDPR portability requirements by requiring data holders to make non-personal content retrievable to the individual. It leads to an infinite scope, impossible to engineer, while bringing no/ very limited added value to the individual.
- The reference of virtual assistants in the EU Data Act should be more careful assessed as it might create legal uncertainty as well as privacy and security risks for consumers. In more detail, the EU Data Act:
    - in light of the broad definition of "virtual assistants", 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 3P 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).
    - is disproportionate to the Act's stated goals which is to enhance competition in the product aftermarket. Virtual assistants don't have a repair or maintenance aftermarkets, only the device that the software runs on have.
    - should not require business to collect and retain more personal data: For example, it requires companies to make "by-products" like data created in stand-by mode available to share with third-parties. However, such data is usually not retained permanently (in fact, it's usually just kept temporarily on the device memory and overwritten every few seconds) and sharing requirements of such data would result in retention of more, often very sensitive data, thereby standing in contrast with data minimisation principles of the GDPR.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

FRAND and unfair contractual terms (chapters 3 and 4)

- The Data Act allows the data holder to be compensated for making data available to a third party pursuant to a user's request. The compensation measures for data sharing between data holders and data recipients provided in Article 9 of the Data Act causes a certain level of ambiguity which could lead to unintended legal fragmentation with the current data protection framework. It is unclear how Article 9 provisions interplay with the right to data portability under Article 20 GDPR. Article 9 of the Data Act clearly foresees some form of compensation for data holders. However, Article 12(5) GDPR requires any actions taken pursuant to a data subject request to be free of charge (unless they are manifestly unfounded or excessive). While the prior mentioned GDPR provisions prevent data holders from charging a fee to the data subject, it is not clear whether this would prevent data holders from charging a fee to the data recipient in the context of a request to port data pursuant to Article 9 of the Data Act.
- More clarity should be provided re: "good commercial practice in data access and use" and "unilaterally imposed" in this context. The lists of conduct that is always unfair and presumed unfair should be further specified to ensure legal certainty.
- 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, given it is much easier to prove something is discriminatory or has happened than it is to prove that it is not or has not happened. The legislative objective can be achieved by the data holder bearing the burden to prove its terms are reasonable. It should then be for the complainant to prove that they are nonetheless discriminatory as they will be the party holding the best evidence. Similarly, a MSME is best placed to evidence that they did attempt to negotiate terms (i.e. that the terms were unilaterally imposed).

B2G data sharing (chapter 5)

- We welcome the intention to harmonize the legal framework on B2G data sharing but the current text could lead to unintended consequences. The proposal doesn't seem to take into account fairness, transparency, reasonableness, and non-discrimination and doesn't include safeguards for privacy, security, protection of business secrets and IP.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Government entities would be allowed to request access to data with relatively light justifications - i.e. not being able to access the data through other means - and with no limitations or safeguards in place. We think the B2G provisions need to be more balanced and take into account the potential risks of data sharing for all the players involved.

- We are also concerned with the broad scenarios of "disclosing data when there's public interest" which could allow broad requests and misuse, as well as security data breaches.

Switching between data processing services (chapter 6)

- We support the Commission's ambition to make portability and switching easier. However, some of the rules seem difficult to implement. For example, the proposal suggests an unrealistic 30-day deadline (extendable to max 6 months) for switching, regardless of the volume and specifications of the workloads at hand. In practice, moving large amounts of workloads sitting across multiple hosting servers can easily be multi-year projects for the larger contracts.
- There is also a question on 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.
- The law requires providers to remove "commercial, technical, contractual and organisational obstacles" but doesn't define what those are and does not introduce any nuance. There could be technical obstacles that are inherent to the switching process and cannot be removed.
- 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. It seems the rules should only apply to removing obstacles under the outgoing provider's control. Providers should have the freedom to innovate and create new features, which will not necessarily map to other systems. We think these measures need to include more nuance and take into account the reality of the provision of cloud services.

Access by foreign authorities (chapter 7)

- The proposal around foreign jurisdiction and government access risks creating more conflict of law by creating a parallel framework to the existing one for personal data. It is unclear how the Data Act would align with ongoing work around Privacy Shield and the CLOUD Act agreement and how success on those fronts would reflect on the Data Act.
- The focus on non-personal data doesn't seem appropriate, as on the cloud information is not stored/processed separately from personal data. It is also 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.
- Even if the article is not meant to restrict data transfers, in practice it may become an obstacle to using global cloud services. The lack of clarity on its application is such that it might discourage customers from using a global service if they are worried about their own compliance with the Data Act. We encourage legislators to clarify the intended objective of this provision, as it is currently unclear how this advances the objectives of the Data Act.

Interoperability (chapter 8)

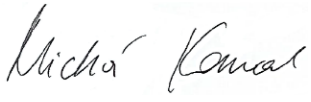
- Interoperability specifications and European standards should be developed in consultation with industry and other stakeholders. They should also reflect existing international standards and industry practices.

Implementation and enforcement (chapter 9)

- There is a potential for tension between the GDPR one-stop-shop mechanism (for personal data) and national enforcement (for non-personal data).

We remain at your disposal at a later stage of the above-mentioned regulation.

Respectfully,
Michał Kanownik



President
Digital Poland Association