Developers Alliance's position on the European Commission's proposal for a regulation on harmonized rules on fair access to and use of data (Data Act)

General remarks

Free-flows of data within the Single Market and beyond are essential for the development of the EU's digital economy. Instead of tackling the root causes of the existing barriers to data flows, the Data Strategy (which the Data Act is part of) is trying instead to artificially intervene in the economy and shape markets around data use. The strategy is based on misconceptions of data.

As emphasized in our positions on the Data Strategy and on the Data Governance Act, the proposed approach is raising many legal and technical challenges, adding another layer of complexity to the EU regulatory landscape. Our main concern is that the obvious outcome for companies and ambitious entrepreneurs, such as software developers, is a higher cost of doing business in the EU and a deterrence against innovation processes and investments.

In particular, the Data Act proposal:

- mandates data sharing while adding more legal uncertainty for all market players, excessive liability for data control, and increasing safety and security risks
- sets ambiguous legal terms for international non-personal dataflows, risking to isolate European digital businesses from their trading partners and the global economy
- aims to encourage the development of aftermarket services and business models dependent on access to assets of other businesses (mainly very large ones) instead of creating the environment for innovation-driven entrepreneurship and growth
- clearly lacks the essential commercial incentives for the viability and success of any economic ecosystem, reducing the potential of the European digital economy

Unintended consequences of the regulation:

- increased threats to users´ privacy and security
- forced asset/IPR transfer to malicious actors and competitors, including foreign state-backed companies
- devaluation of the value of data capture
- reduction of data-intensive/reliant investment in the EU.

Related data-driven ecosystems naturally created by the free market represent the sole viable ways to reap significant benefits of the digital economy. The proposal is going against this and therefore we are skeptical about its promised benefits.

On the scope (Chapter I)

The scope of the regulation, as derived from the definitions of “data” and “product” (art. 2.1 and 2.2) is broad and unclear.

There is no specification in relation to personal data, as defined by the GDPR, versus non-personal data, considering the prevalence of mixed datasets.

The regulation is intended to apply to “data recipients in the Union” and users of products and services placed on the EU market, without specifying that these should be legal or natural persons under EU’s jurisdiction (art. 1.2.b),c),e), art. 2.5 and art 2.7)

The definition of “related service” should be corrected, as all digital services involve software (art.2.3).

The notions should also be correlated to the terminology already laid down by relevant EU law, especially the GDPR (e.g. data holder - data controller).

On B2B and B2B data sharing (Chapters II, III and IV)

The obligations to provide data sharing by design should be complemented by robust safety and security by design. Meaningful transparency for users is very important and the related provisions should be correlated with existing obligations in this sense. (art. 3)

The right of users to access and use data generated by the use of products or related services is more than an extension of GDPR’s data portability, it seems to be an entirely new right. It comprises access to non-personal data and information which are not clearly defined. It is also unclear what is the state of data protection in the situation of data shared by the users to 3rd parties which could transfer the data further on. For legal certainty, the users’ right of access and use should be maintained within the limits set by the GDPR. Moreover, users’ informed consent could be problematic, due to the fact that they cannot anticipate and have proper knowledge of whom they are giving access to their data.

User authentication should be as easy as possible, but also a strong process, especially for personal data protection. Also, the implementation of the data minimization principle needs to be balanced with essential measures for ensuring cybersecurity. (art. 4.2 and 5.3)

The broad scope of the proposal and unclear conditions for data sharing pose high cybersecurity risks.

> *For example: In the case of diagnostics data, such information is oftentimes unstructured. It is obviously very difficult for users to understand and therefore difficult to manage such data. When average users, with limited or lack of knowledge how to manage such data, share it with third parties, there is a high risk that the information will be easily abused by bad actors. Those could potentially analyze and use it for purposes that users were not aware of, or could potentially find ways to hack the devices and thereby compromise users' overall security.*

The proposal sets very weak safeguards against disclosure of trade secrets. Also, the level of protection is uneven depending on the data recipient (1st party users/3rd parties), without justification. Without proper amendment, such provisions will put a variety of companies under the risk of losing their competitive advantage and will be strong disincentives for future investments in the EU economy (art. 4.3, 5.8 and 8.6). It is essential to include stronger legal safeguards, including direct references to the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

The poor safeguard of trade secrets is also complemented by weak obligations for 1st party users and 3rd parties not to use the requested data "to develop a product that competes with the product from which the data originates" and also for 3rd parties not to "share the data with other third party for that purpose". (art. 4.4 and art. 6.2.e)

There should be severe consequences, besides the usual judicial recourse, for unauthorized disclosure of trade secrets for a product and related service, as well as confidential business information.

Legally it will be complicated for companies to protect their assets and innovation prospects. For example, they will heavily depend on relevant national authorities and the courts' interpretation of what qualifies as a "competing product". Considering also that the definition of users does not specify that they are under EU's jurisdiction, as well as the 2rd parties, such provisions are thus unenforceable for many situations.

> *For example: A state-backed foreign company could easily have access to trade secrets of an European company (which could be active in the defense sector as a manufacturer of dual-use products). It is enough to operate as an user of industrial IoT products or as a provider of aftermarketing services within the EU.*

The proposal arbitrarily adds to the rigid approach of the DMA more constraints for providers of digital ecosystems designated as "gatekeepers". (art. 6.2.d). The restrictions for data flows covering a wide-range of services provided by these companies are not justified and supported by a proper impact assessment on the impact on those ecosystems, including on consumers options. It is just another bad signal for business growth and investment in the EU.

> *For example: Many software developers use business services provided by large online platforms. They also provide apps across jurisdictions. If a data service used for the development or maintenance of an app is not available anymore in the EU, there will be a direct impact on the app availability in the EU.*

Regarding the proposed threshold for B2C and B2B data sharing, while it relieves them from regulatory burdens, it doesn't serve ambitious entrepreneurs, startups, which will be discouraged to grow. It's also unclear how it serves consumers, whose rights seem to be limited depending on the size of the company they interact with. This makes the objectives of the regulation questionable. (art. 7.1)

The provisions setting the conditions for data holders to make data available raise questions on the correlation with applicable civil and commercial law at Member States level. Furthermore, given the

broad scope of the regulation, the proportionality in relation to the freedom to conduct a business and freedom of contract is also questionable. (art. 8-13)

On the compensation for making data available to third parties, the interplay between art. 20 GDPR and the possibility to set the compensation according to FRAND terms should be clarified. As the definition of ”data” is very broad, it is legally uncertain how it correlates with the data protection framework and how it will work in practice (art.9).

Overall the regulation offers poor legal safeguards for data holders to protect themselves from those that can easily abuse the system. The users, especially the natural persons, can be easily manipulated by bad actors which would push the legal limits from the privileged position the regulation offers them.

Also, the regulation’s approach seems to be constructed based on simple situations, ignoring the variety of situations that would fall under the scope, including complex value chains and business relationships. In practice, such situations (which also usually involve mixed datasets), will be covered by a convoluted legal framework. It could be very difficult to identify the distribution of obligations and liability, which before was governed by contractual terms in accordance with the GDPR and other applicable laws, as the case. The regulation adds unclear obligations which would discourage companies to participate in complex projects, engage with multiple business partners or develop complex products and services.

> *For example: Software developers often participate in ecosystems, providing various applications or software components.They might not be necessary all the time in a sole business relationship with a big company, but part of a value chain or complex project, interacting with various partners of different sizes and levels of implication. They need legal certainty with regard to their obligations and liability.*

On B2G data sharing (Chapter V)

The objective of setting a clear framework for B2G data sharing is salutary. However, stronger safeguards for privacy, security, protection of business secrets and IP should be ensured to avoid abuses and unintended consequences.

The risks for personal data protection should be mitigated by a strong correlation with the GDPR and by adjusting the conditions for mandatory data sharing and the obligations for public sector bodies and Union institutions. For example, a broad scope allowing authorities to ask for data whenever they appreciate that they’re unable to obtain it, could lead to excessive government access to personal data without proper justifications and necessary safety and security safeguards. Such scenarios are exceeding exceptional circumstances, empowering governments to routinely impose data disclosures (including personal data) (art. 15.c)

In the same vein, the risk of misuse and data breaches are increased by the re-sharing of data by public sector bodies and Union institutions with 3rd parties (such as individual researchers or organizations), for a wide array of reasons. The title of the article specifying “in the context of exceptional needs” is in obvious contrast with the broad scope of the provisions. (art. 21).

On switching between data processing services and interoperability (Chapters VI & VIII)

While the customers of data processing services may appreciate easier ways to switch and avoid lock-in effects, the conditions for switching and portability need to be realistic. Again the scope of the regulation is broad and covers many different situations. For example, the deadlines might be viable for certain customers, but in the case of large data volumes, multiple applications and digital assets, distributed across several hosting servers, covered by complex contractual arrangements, these might not be reasonable. Also, when it comes to technical conditions, the requirement on ensuring "functional equivalence" seems to imply that the data processing services should operate on standardized systems. This is also unrealistic, as cloud services might differentiate and compete based on different features they offer. (art. 23, 24)

In addition to the prescriptive approach for deadlines and other contractual terms, the price intervention and monitoring of private services represent a disproportionate government intervention in the market. (art. 25)

Concerning the essential requirements for interoperability, we strongly recommend maintaining the presumption of conformity approach. Common specifications elaborated by the Commission should not be imposed as a compulsory means for conformity instead of voluntary standards, based on industry best practices. Also, the European standards should be aligned with the relevant international standards and involve different stakeholders in their development. (art. 28.5.6)

It is not clear why there is a need for a declaration of conformity for smart contracts. The observations above on the standardization approach are valid for art. 30 too.

On international non-personal data flows (Chapter VII)

It is unclear what is the objective of the provisions on international access and transfers.
As mentioned above, the weak safeguards for mandated data sharing entail a high risk for allowing bad actors, such as state-backed foreign companies to have access to data and trade secrets. It seems that those risks were ignored, while specific provisions are tackling unclear concerns regarding cloud services.

Art. 27 is adding unjustified legal uncertainty on exchanges of non personal data, which translates into unilateral restrictions to data flows. This will disrupt how many European businesses currently work with their subsidiaries, partners, suppliers and vendors, and undermine European players' efforts to scale up outside Europe.

We encourage the European Commission to address legitimate concerns about foreign governments data access with like-minded third country governments, alongside EU Member States. With regard to personal data, the bilateral discussions between the European Commission and the US Administration on a stable solution for transatlantic transfers are highly relevant.

Another source of legal uncertainty on data flows, on non-personal data, in addition to the already complicated situation for personal data, could have important consequences for the European digital economy. The EU Single Market should remain open to trade.

On the sui generis right under the Directive 96/9/EC on the legal protection of databases (Chapter X)

The proposal imposes a broad restriction of the scope of the sui generis right.
Instead, art. 35 should specify if the sui generis right does not apply when it is in conflict with the rights of users to access and use data (art. 4), respectively with the rights of users to share data with 3rd parties (art. 5).

In the spirit of the Directive 1996/9/EC, it should be also specified if the sui generis right is applicable when the databases containing data obtained or generated by the use of a product or protected device were subject to substantial investments related to the verification and displaying of the data.

On implementation & enforcement (Chapters IX & XII)

As the scope of the regulation covers both personal and non-personal data, the implementation and enforcement should be better correlated with the GDPR one-stop-shop mechanism. Moreover, it should be clarified the role of the DPAs and how they will work together with the designated competent national authorities.

The risk of fragmentation should be mitigated by strong cooperation between Member States.

The regulation was intended as a horizontal legal framework, but art. 40.2 shows that far reaching requirements exceeding this framework could be adopted on a sectoral basis.

Moreover, recital 79 indicates that the Commission intends to furter adopt common specifications as a replacement for voluntary harmonized standards. This approach will not be beneficial for innovation in the EU and risks imposing trade barriers if the EU is ignoring industry best practices and relevant international standards.