EU REGULATION ON HARMONISED ON FAIR ACCESS AND USE OF DATA – DATA ACT

INTRODUCTION

The Federation of European Data and Marketing (FEDMA) shares the objectives of the European Commission to increase access to and further the (re-)use of data through the proposed 'Data Act'. Access to customer data is extremely important in the Data and Marketing sector. Data allows marketers, especially SMEs, to reach in a cost-effective way the right audience with relevant and personalised offers of their products and services which often represent alternatives to well-established brands and large commonly known online platforms. Marketers do not only use consumer data to increase the efficiency of their marketing spend, but also as a source of innovation to deliver new value and enhanced products and services for customers.

Data sharing in the Data and Marketing sector mostly takes place via data intermediaries, which collect consumer data and provide them across business partners, in line with the EU data protection framework. For instance, a telecom company makes available aggregated location data from its mobile phone users to a chain of hotels and restaurants in a particular country, allowing these companies to provide customers and prospects with relevant advertisements, offers and discounts based on their location.

Considering this background, FEDMA believes that the Data Act proposal can play an important role in enhancing data sharing across markets benefitting both individuals and businesses. As a key pillar of the European Data Strategy, the Data Act should provide legal certainty, thus enabling the industry to easily comply and reap the benefits of the new Regulation. FEDMA also believes that the Data Act should keep an approach which ensures coherence with other legal frameworks, especially the General Data Protection Regulation (GDPR), and refrains from creating undue friction in international data flows.

Specifically, we recommend:

1. Clarifying the scope of the Data Act proposal in relation to the definition of "data" and "related services".
2. Clarifying the interplay between the definition of "connected product" and the concept of "terminal equipment" in the ePrivacy Directive (forthcoming ePrivacy Regulation).
3. Aligning the sharing and reuse of the user's personal data within the framework set by the GDPR, thus refraining from creating further restrictions overriding the existing body of EU data protection law.
4. Including the use of pseudonymization and anonymization as appropriate privacy-preserving measures.
5. Simplifying the provision of pre-contractual information to the user.
6. Narrowing the definitions of "public emergency" and "exceptional need" to ensure legal certainty in Business-to-Government (B2G) data sharing.
7. Removing requirements on international transfers of non-personal data which are not proportionate to their lower level of risks compared to personal data.
8. Ensuring fair contractual terms without jeopardizing the principle of contractual freedom.
9. Refraining from setting prescriptive requirements and standards on smart contracts due to the early development of this technology.

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

1. Clarify the definition of "data" and "related services"

We believe that the definition of data is unclear as it seems to vary throughout the proposal. In particular, while Chapter II seems to exclusively target Internet-of-Things (IoT) data generated by connected objects, the provisions on Business-to-Government (B2G) data sharing and international data transfers seem to apply to any type of data from the private sector. If this distinction was part of the intention behind the proposal, FEDMA recommends clarifying this delimitation.

FEDMA also voices concerns about the proposed definition of "related services" which could benefit from further clarification. The Data Act should indeed target those best placed to give access to the IoT data directly generated by connected objects, namely, the manufacturers. However, the current definition of "related services" risks broadening the scope beyond the manufacturers, failing to delineate responsibilities between stakeholders in the supply chain. It is unclear whether "related services" also refers to data services using data generated by a connected product, but not directly sold with the product itself by the original manufacturer. For example, services developed by third party service providers based on data generated by tags, such as temperature or humidity. While the objective of the proposed Data Act is to promote the development of Data Economy by increasing the number data-based services and service providers, a too wide definition of "related services" will hamper this development. Instead, we believe the current definition should exclusively refer to additional web-based interfaces, sold or rented together with the connected product, which allow the user to benefit from additional features of such product.

2. Clarify the interplay between the definition of "connected product" and the concept of "terminal equipment" in the ePrivacy Directive

Recital 14 of the Data Act proposal explains that the new rules broadly apply to connected products in the area of the Internet of Things (IoT) such as smart home appliances, smart industry machines, etc. Conversely, products primarily designed to display, play, record or transmit content (e.g. personal computers, servers, smartphones, webcams, etc.) shall not be covered by the Regulation. Yet, current technological developments risk blurring the line between these two categories. It remains unclear, for instance, to what extent a personal computer or a smartphone used to operate the connected product while also generating data will fall under the scope of the proposal. In this context, we believe it is fundamental to clarify the interplay between the definition of "product" under the Data Act with the concept of "terminal equipment" in the ePrivacy Directive[1], and whether or in which cases the ePrivacy rules requiring consent for use and access of data would apply to a connected product.

3. Aligne the sharing and reuse of the user's personal data within the framework set by the GDPR

The Data Act specifies that the new rules are without prejudice to the GDPR (Recital 7) and complement Article 20 GDPR (Recital 31), granting "*users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing*". Nevertheless, the proposal seems to go beyond the level of protection of the GDPR, raising unnecessary additional barriers to personal data sharing.

Specifically, the prohibition under Article 6(2)b whereby third parties cannot use IoT data for profiling purposes, unless necessary for the service requested by the user, unfairly restricts the user's right to data portability as Article 20 GDPR does not limit profiling to the sole ground of "necessity". Instead, in contrast

[1] Any equipment which is connected directly or indirectly to the interface of a public telecommunications network to transmit, process or receive information

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

to the GDPR, the Data Act proposal prevents the user himself from further sharing personal data for purposes other than the fulfilment of the agreement with the third party, on the basis of other GDPR legal bases, including consent and legitimate interest. Article 6(2)b would thus undermine the objective of user empowerment, curtailing the user's freedom to share his/her data.

In doing so, this interdiction would also prevent third parties from reusing personal data in a GDPR-compliant way for purposes other than the fulfilment of the agreement with the user. In the Data and Marketing Industry, for example, profiling, or assigning consumers to different audience groups, is not only fundamental to provide personalised offers to a specific individual and build a customer-brand relationship, but it is also crucial for the effective training of algorithmic models for the development of new innovative products and services.

Article 6(2)c also conflicts with the objective to foster data sharing within the framework of the GDPR as it prohibits the third party to share the data with another party "in raw, aggregated or derived form unless this is necessary to provide the service requested by the user". Access to third-party data is crucial for many organisations in the Data and Marketing Industry to compete with larger players who have direct access to a large pool of first-party data. The proposal thus seems to fail to take into consideration Privacy Enhancing Technologies (e.g. pseudonymisation or anonymisation) which could enable the safe sharing of data across multiple parties in compliance with the GDPR.

In addition, the impossibility for the third parties to reuse the data for profiling purposes or to make it available to other organizations will also have the effect of limiting the possibility for economic actors to use the data in order to train algorithms of artificial intelligence. Data access and profiling are indispensable elements for effective training of algorithmic models. These restrictions therefore appear contrary to the objective sought by the DA to promote highly strategic technologies such as artificial intelligence systems, an area "whose full potential the EU has yet to harness" (see explanatory memorandum – page 7).

With the GDPR, the EU has set up a modern data protection framework which establishes a satisfactory balance between companies' interests and the protection of individuals' fundamental rights. As such, other jurisdictions around the world have recognised the GDPR as a global standard which they took as a model for their national data protection legislations. Yet, proposals like the Data Act which set further restrictions on the application of the GDPR, undermine these achievements and the credibility of the GDPR as a future-proof framework fitting different data uses and data-driven business models.

In this context, FEDMA calls for better aligning the Data Act provisions on the processing of the users' personal data with the GDPR, taking into consideration all different legal bases under Article 6(1) GDPR in combination with additional safeguards, including pseudonymisation and anonymisation techniques. This approach would also strengthen the consistency with Article 20 GDPR on the right to portability as well as the objectives of the Data Act proposal "to facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data".

More generally, FEDMA would like to nuance the EDPS/EDPB's position[2] in their opinion on the Data Act that the "*text would extensively push a "commodification" of personal data, whereby personal data are seen as a mere tradeable commodity […] that would risk undermining the rights to privacy and data protection as fundamental rights*" (see paragraph 15). Data has long been considered as economic asset. This should not be seen as preventing its protection according to the framework set up by the GDPR – as evidenced by the emergence of data-driven businesses in several economic sectors, in full

[2] EDPS-EDPB Joint Opinion on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

compliance with the GDPR. Reaping the value of data to drive innovation and growth in the EU while protecting data protection rights is indeed the objective of the Data Act and the European Data Strategy.

4. Include the use of pseudonymization and anonymization as appropriate privacy-preserving measures

IoT applications collect and generate significant volumes of data in order to perform properly while also improving their service and developing new products. Though these data-driven characteristics of IoT products and services can pose risks to the user's privacy, we believe the Data Act proposal should promote the use of existing mitigation techniques to safeguard the sharing and (re)use of users' personal data, thus promoting access to data and value creation. Provided as an example of an appropriate data protection safeguard by the GDPR, pseudonymization is, for instance, a foundational technique to mitigate these risks by replacing private identifiers with fake identifiers or pseudonyms to hide key identifiable information. In contrast to the current text, the Data Act should thus allow a third party to reshare the user's personal data in a pseudonymized format with another party, whereby the former would safely keep any additional information which could enable the latter to re-identify the user: the data in question for the other party would thus be considered anonymous.

In this regard, anonymization represents another valuable privacy-preserving mechanism in case the data in question is personal data, and FEDMA believes it would be a missed opportunity for the broader EU Data Strategy, should the Data Act not leverage it to foster data sharing in a secure way. A typical practice in the Data and Marketing Industry, for example, is to anonymise personal data by means of data aggregation. In this case, the data in question is considered anonymized when aggregation is carried out on at least 10 persons. Nevertheless, should data aggregation not be possible, there are alternative measures of anonymization, often used for data-driven marketing, which can be taken and leveraged in the context of IoT applications, including:

- Generalization: values made into categories. For instance, instead of having a field "age", create a field "age group" that shows age in age-bands such as "below 20" "20-40" etc.
- suppression/deletion: avoiding the use of attributes[3] that can be used to select less than 10 records).
- Differential privacy: the addition of randomised noise or "fake data" to the database to protect individual records

FEDMA therefore recommends including the use of pseudonymization and anonymization techniques as "appropriate technical protection measures" in Art. 6(2)n, Art.6(2)c and Art.11.1. This will allow to better align the Data Act with the GDPR rather than establishing additional restrictions which would hinder the European data strategy's general objective of access to data and value creation.

5. Simplify the provision of pre-contractual information to the user

While FEDMA agrees with the Commission's approach to provide users with relevant pre-contractual information, we believe some practical implications of such information will raise significant legal uncertainty. In particular, the provision of precise information regarding the "volume of data likely to be generated" (Art.3(2)a) seems rather unrealistic as this will depend on whether the user is a natural or legal person and on the way the user will make use of the product or related service. It is therefore unclear the added value of providing the user with such information where this is only going to consist of a general and vague range of volume. As such, we recommend removing this requirement.

[3] Attribute = also referred to as data elements. This is information used to describe the often unique characteristics ascribed to an identifier. Examples include "gender," "has a cat (y/n)," "hobby is skiing (y/n)."

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

6. Narrow the definition of "public emergency" and "exceptional need" in B2G data sharing

In light of the abovementioned unclear definition of data in respect to Chapter II, the scope of the provisions on mandatory Business-to-Government (B2G) data sharing risks raising significant legal uncertainty, potentially including organisations other than the IoT industry. This lack of clarity is further aggravated by the overly broad definition of "public emergencies" and "exceptional needs" which could be subject to multiple interpretations. In particular, as an exceptional need may not only exist when the requested data are necessary to respond to a public emergency, but also where the lack of available data prevents the public authority from performing a specific task in the public interest, the thresholds for public sector bodies to access "data" are extremely vague, potentially leading to the abuse of this right of access without necessary safety and security safeguards which could expose commercially and privacy sensitive data.

In this context, FEDMA reiterates the EDPS/EDPB joint opinion, urging EU legislators to define "much more stringently" what qualifies as a 'public emergency' and 'exceptional need'. In order to ensure that access to data by public authorities remains limited to what is strictly necessary and proportionate, while also strengthening transparency and trust, we also recommend requiring public sector bodies to

- provide data holders with information on the security measures for the requested data,
- clarify the reason whereby the lack of data would prevent a public sector body from fulfilling a task in the public interest
- share information on how the data made available were used.

Finally, we believe that data holders should have the possibility to request either a modification of the request submitted by a public sector body or a Union institution, body or agency, or its cancellation within 5 or 15 working days depending on the nature of the exceptional need invoked in the request.

7. Refrain from setting requirements for international transfers of non-personal data disproportionally to their level of risk

The Data Act provides that where international "transfer" or "governmental access" to non-personal data held in the EU "*would create a conflict with EU law or the relevant national law*", providers of data processing services shall take all reasonable technical, legal and organisational measures to prevent such transfer or access. FEDMA believes that these provisions raise significant concerns not only due to their lack of clarity on what constitutes 'legal, technical and organidational measures', but also for the risk of creating undue tensions in international data flows in addition to the increasingly complex framework for the international transfer of personal data.

As such, the Data Act proposal might burden companies' ability to transfer a type of data that carry lower risks compared to personal data. The invalidation of the EU-US Privacy Shield and the revision of the Standards Contractual Clauses (SCC) have stressed the need for businesses to constantly undergo significant organisational and financial pressure to readjust their personal data transfer practices. While the sensitive nature of personal data can justify the need for a prescriptive data transfer regime, the safeguards for transfers of non-personal should also be proportionate to the risks they aim to address.

In this context, though the Data Act provisions only target cloud service providers, many European businesses relying on those services to scale up outside the EU will be adversely affected by such new source of legal uncertainty on data flows.

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

8. Ensure fair contractual terms without jeopardizing the principle of contractual freedom

As underlined in the Data Act proposal, a stronger bargaining position on the data holder side can lead to unreasonable conditions for sharing the data at the detriment of the data recipient which can thus be left with no other choice than to accept 'take it or leave it' contractual terms. In the Data and Marketing Industry, these situations occur in regard to voluntary agreements across business partners who share individuals' data, within the framework of the GDPR, to use the information for their own direct marketing purposes.

The combined implementation of the Platform-to-Business Regulation and the forthcoming Digital Markets Act is already expected to partly address this issue, especially in the context of marketing communications based on digital advertising, but their benefits would be limited to agreements where the data holder is a platform or a gatekeeper.

As such, the Data Act proposal could bring an additional element to avoid unilateral changes of contractual terms, disproportionate restrictions on the use of data, limitations in the termination of contract, etc. Nevertheless, we are concerned that the prescriptive nature of the FRAND provisions in the Data Act may have an adverse impact on contractual freedom and lead to abusive use of these provisions, as well as rapidly become obsolete. Instead, we recommend EU legislators favour principle-based rules to strike the right balance between fair access to data and contractual freedom. Failing such a balance, the provisions may constitute a disincentive to share data, whereas the objective of the Data Act is to incentivize data sharing.

9. Refrain from setting prescriptive requirements and standards for smart contracts

FEDMA welcomes the Commission's pro-innovation approach to promote "smart contracts" as a reliable tool in the context of an agreement between a data holder and a data recipient. As a core application of blockchains, the use of smart contracts in the Data and Marketing Industry is increasingly being explored for the self-execution of deals in the supply chain. Use cases range from data sharing across intermediaries, addressing ad fraud issues, to maintain accuracy of inventory, to better connect consumers with brands, as well as improving consumer privacy. However, FEDMA believes that the Data Act's smart contract requirements and the Commission-prescribed standards are excessively premature, considering the early stage of smart contracts development and scaling, and would rather hinder innovation, especially in the field of blockchain and other smart contract related initiatives.

***

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org