Position paper on the EU Data Act

1. Introduction

Ecommerce Europe welcomes the European Commission's ambition to remove barriers to access data and encourage data sharing, while preserving incentives to invest in data generation. The availability of greater amounts of data, along with improved access, emerging analytics tools, and state of the art technologies, will allow European businesses to better leverage the data they already possess while improving outcomes through enhanced collaboration with international partners to advance Europe's digital goals and global competitiveness. We recognise the growth potential of the EU data economy and would like to point out that extensive data sharing already occurs in the digital commerce sector. However, Ecommerce Europe believes that the Data Act will only be successful in reaching its objectives as long as its obligations will not be overly restrictive and technically feasible for businesses in Europe.

2. Scope & Definitions

Article 1 of the Data Act lays down the scope of the Regulation. The rules are intended to cover all sectors, all actors in the supply chain and all interactions (B2C, B2B and B2G). In order to apply these rules correctly, it is crucial to provide further clarity on the scope and better clarify the role of each player as regards the new access rights put forward by the Data Act. The current text, rather than clarifying, risks creating ambiguity, whether protections for customer data and trade secrets are weakened. Ecommerce Europe would argue that a more targeted approach, focusing on data generated by IoT products and related services, is more appropriate. Given the diversity of the various sectors, which each have a distinct ecosystem, we think sector-specific legislation would be better suited to address targeted concerns. We firmly believe that policymakers should only regulate what is necessary, and not attempt to overregulate sectors which are not experiencing difficulties.

It is instrumental for the economic operators falling within the scope of the proposal to be aware of the role they fulfil, the type of data that is to be shared and with whom. Therefore, further clarity is also needed on the following key definitions of the proposal:

Data

The proposal is not consistent in the type of data affected under the various articles. Some articles are focused on data generated by the use of the products or related services, but other articles appear to refer to all potential data being held by a data holder. The definition of data needs to fit all chapters of the Data Act, including the articles on data access and sharing as well as on government data access. Moreover, the types of data covered by each section should also be clearly stated. Some provisions specifically target non-personal data, for instance for restrictions on international data transfers, but in other cases it is unclear how the text relates to personal data already covered under the GDPR, for instance for personal data in an IoT context. In any case, the relation between the GDPR's Article 20 on data portability and the Data Act's Articles 4 and 5 on right to access and share data should be clarified. Additionally, the distinction between user-generated and product-generated data should be better defined. The difference between non-processed and processed data and between data aggregated by IoT or data aggregated by the data holder should also be clarified. According to the recitals, the proposal is intended to cover only raw data and derived data and inferred data should not be shared. It would be helpful to have increased clarity on the type of data that needs to be shared and not only what should be excluded.

Data holder/user

For the retail industry specifically, it is crucial to ensure that the definitions of the various economic operators in scope of this proposal are clarified. The current text leaves confusion over the distinction between data holders and data users (and even data recipients), making it uncertain in which cases retailers could be considered as data holders and/or users. Additionally, the concepts of data holder and user are unclear in relation to the concepts of data processors and controllers under the GDPR. For instance, recital 24 states that "insofar as personal data are processed, the data holder should be a controller under Regulation (EU) 2016/679", but for non-personal data, Article 2(6) states that the data holder can be any legal or natural person that "through control of the technical design of the product and related services, [has] the ability, to make available certain data". The difference between how a data holder should be understood for personal and non-personal data complicates the application significantly. Especially as in reality there are often many different businesses involved in complex ecosystems of "products" and "related services", where several data processors could all be considered data holders, at least for part of the data, but not all of which will have a contract with the user. This could be clarified by limiting the definition of "data holder" to exclude infrastructure or software providers and other parties who may be contractually prohibited from producing the data and would help ensure that parties can agree compliance obligations through contractual arrangements. It is important to clarify the definition of a data holder for non-personal data, and ideally to align the definitions used to the already existing concepts of data processor and data controller. Finally, the confusion also extends to the lack of differentiation for the use of the concept 'data user' in a business-to-consumer (B2C) and a business-to-business (B2B) context.

Product

Article 1.2. remains rather vague on the products that are covered by the proposal. Recital 15 provides further information, but this should be better reflected in the article. Ecommerce Europe would encourage the Commission to use the definition from the report on the sector inquiry on IoT.

3. Business to Consumer and Business to Business Data Sharing

Ecommerce Europe welcomes the Commission's intention to increase and facilitate data sharing for IoT devices and related services. We recognise the potential of data sharing for enabling growth and innovation. We also agree that steps can be taken to improve transparency and access to data generated by users to create a more competitive and innovative market. However, we question whether the proposed approach is the most suitable to achieve the desired result.

Currently, B2B data sharing occurs through voluntary agreements between companies based on the principle of the contractual freedom. Obstacles could occur when companies decide to enter into a data exchange, such as a lack of trust in how the data is being treated and whether privacy will remain protected and concerns that investments in data innovation are not undermined by disclosure of trade secrets. While we believe these issues could certainly be addressed to stimulate B2B data sharing, the first three chapters of the proposal go much further than providing incentives and instead require access and use of all data (personal and non-personal) generated by IoT devices for users, and user-designated third parties. Ecommerce Europe finds this right to data access in the current proposal too broad and stresses that the goal of the data act should be to incentivise data sharing and in no case deter companies from offering or developing IoT solutions.

Article 3 states that before "concluding a contract for the purchase, rent or lease of a product or a related service" certain information on the data shall be provided to the user, in a clear and comprehensible format (e.g., the nature and volume of the data likely to be generated by the use of the product or related service;

how the user may access those data; whether the manufacturer or the service provider intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used). It is however unclear to whom this obligation refers: the text does not mention whether it is the manufacturer, the service provider or if this could even be the retailer as this is a precontractual information requirement. Additionally, if the data collection changes after a contract has already been concluded, what impact would that have on the rights of the user?

Articles 4 and 5 address the protection of trade secrets. Ecommerce Europe strongly suggests ramping up the safeguards for trade secrets to ensure that incentives for innovation remain. Additionally, the proposed rules seem very difficult to enforce. For instance, how could a data holder be certain that "all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties" (Art. 4.3)? Further details are also needed on what such "specific necessary measures" would entail. This could be addressed by clarifying explicitly that there is no obligation to share trade secrets in relation to Chapter II. This would not prevent companies from sharing information confidentially if they choose to do so and provided the appropriate safeguards, as they deem fit, are in place.

Article 4.6 states that the data holder shall only use non-personal data generated by the product or related service as contractually agreed with the user and will not be able to use these data to derive insights about the user that could undermine the commercial position of the user in the markets in which the user is active. It should be clarified what is meant with 'commercial position' to avoid creating legal uncertainty for both user and data holder. Additionally, this provision appears to go beyond what the GDPR prescribes for personal data, which includes the possibility to use data based on legitimate interest.

Article 5 excludes companies that have been designated as 'gatekeepers' in the Digital Markets Act from benefitting from the data access rights established in chapter II of the proposal. Ecommerce Europe recognises that under specific circumstances the Data Act may risk reinforcing entrenched market positions. Against this background, a mechanism to address this risk is welcome. However, the proposed blanket exclusion of gatekeepers from receiving data transfers appears disproportionate given the restriction of the freedom of choice for end users this entails. Rather, Ecommerce Europe suggests that the Commission's services in charge of the DMA enforcement should be empowered to take a decision to exclude gatekeepers only where objective conditions are met, such as an entrenched position in relevant product or service markets.

Article 6.2(e) prohibits third parties from using the data they receive to "develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose". Ecommerce Europe believes that this prohibition should not only apply to products, but also to services. The investments and R&D for services continue to grow in significance and while the Commission refers to aftermarket services such as repair and maintenance, the data could also be used to develop a service that competes with the primary service offered, which risks lowering the incentives to invest and innovate. The pro-competitive effect of the Data Act would be maintained by the extension to related services, because third parties could still offer a service which could be in competition with a product or related service other than the one the data originated from.

4. Unfair Contract Terms

Article 13 of the Data Act sets out to protect micro, small or medium-sized enterprise from unfair contractual terms unilaterally imposed on them. Ecommerce Europe strongly supports this objective and stresses the importance of supporting SMEs to enable them to play an increasingly relevant role in the EU data economy. While we therefore welcome Article 13 as such, we also recognise that a concept such as "unfair" is difficult to define and risks being interpreted differently by institutions at both EU and national level.

Additionally, it could be quite burdensome for the data holder to have the burden of proving that contractual terms are not unilaterally imposed. Ecommerce Europe welcomes the Commission's commitment in Article 34 to develop and recommend non-binding model contractual terms on data access and use. We believe this could help to support companies, SMEs in particular, to have a stronger position in negotiating contracts with balanced contractual rights and obligations.

5. Business to Government Data Sharing

The last few years, which were marked by the COVID-19 global health crisis, demonstrated the importance for public bodies to receive data in emergency situations. Ecommerce Europe fully understands and supports the need for businesses to share certain data where public health and safety could be at risk. To ensure this, the Data Act proposal mandates data holders to make data available to a public sector body, a Union institution, agency or body, demonstrating an exceptional need to use requested data.

Chapter V appears to apply to any data a data holder holds, making the scope of the chapter much broader than that of chapters I-III, which were limited to connected devices. As mentioned above, Ecommerce Europe understands the need for data sharing in certain situations, but would suggest narrowing down this chapter, preferably by encouraging voluntary agreements between businesses and governments, but at least by providing further clarity and certainty on the conditions and purpose for which data is being shared. Government access to business data should be restricted to situations in which there is a clear 'exceptional need' and be accompanied by safeguards with better protection of trade secrets. To achieve this, Ecommerce Europe believes the chapter needs to provide certain clarifications.

First, Article 15 describes the circumstances under which an exceptional need is deemed to exist. This would be the case if (a) the data is necessary to respond to a public emergency; (b) the data is necessary to prevent a public emergency or to assist the recovery from it; or (c) the data is needed for public bodies to fulfil a specific task in the public interest that has been explicitly provided by law, but only when they could not obtain the data by alternative means and the adoption of new legislative measures cannot ensure the timely availability of the data, or when this would substantively reduce the administrative burden for data holders or other enterprises. In particular Article 15(c) requires further clarification on the situations this would include, which would not already be covered by existing legislation. While the exemption for small and micro enterprises is welcomed, the article remains quite broad and seems to grant quite significant leeway for public bodies to get access to company data. Therefore, further clarity would be helpful to ensure legal certainty for businesses, but also to ensure a uniform application across the EU.

Second, Article 17.4 states that public bodies may exchange data obtained with another public body "in view of completing the tasks in Article 15 or […] in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party." While this principle as such may in some cases be helpful, safeguards need to be in place to ensure that technical protections are appropriate especially with a view to business sensitive data and potentially even personal data (which is not excluded by the article). While the article mentions that public bodies need to notify the data holder about the transmission of data, we suggest clarifying that the data holder is informed ahead of the data transfer and is given the possibility to object. It also should be explained how to deal with situations in which the shared data includes data about third parties. For instance, in the case of e-commerce marketplaces, this could be data about the sellers or customers. There is currently no procedure foreseen to inform these third parties or information provided about the rights these data subjects have.

Third, Article 21 allows public bodies to share data "with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested, or to national

statistical institutes and Eurostat for the compilation of official statistics." It is important to clarify what can be understood as "compatible purpose". Similar safeguards should be introduced as mentioned in the context of Article 17 as businesses need to be able to trust that is protected. Ecommerce Europe suggests excluding commercially and privacy sensitive data from the scope of Article 21.

6. Switching between Data Processing Services & Interoperability

Ecommerce Europe supports the objective of chapter VI to facilitate easier and more cost-effective portability and switching between data services. However, the provisions do not seem to reflect the diversity of cloud services and the volume of the data, both of which often can be technically complex. Moreover, the Data Act proposal places most of the responsibilities for the switching process on the sending service, which is not always realistic. Instead, the Data Act should better reflect the need for cooperation between the exporting and importing data processing service to enable effective switching. The text should also tailor switching requirements more to the specificities of the data processing services involved and better take into account current market practices.

For instance, Article 26 states that providers of data processing services shall ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys "functional equivalence" in the use of the new service. In Article 2(24), functional equivalence is defined as "the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process" for which the "destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service". Ecommerce Europe believes that achieving functional equivalence is not always possible. Cloud services can diverge strongly from one another, even when they generally could be considered the same type, to ensure a competitive position in the market and offer customers different functionalities. Customers choose their data processing service often based on the special features offered. It is impossible for data processing services to have adequate awareness of the functionalities of other data processing services to "ensure" any functional equivalence. This makes the principle of delivering the same output and performance rather difficult and may lead to less innovation and differentiation in cloud services. Moreover, there is no indication of how the original provider would be able to technically ensure this functional equivalence and maintain a certain quality of service without having access to the environment of the new provider. Furthermore, the obligation to switch within 30 days, or 6 months in exceptional circumstances, negates the complexity that can be involved with switching operations. Contracts between data processing service providers and customers should therefore include the right for the latter to request or agree to a longer transition period.

The Data Act proposal proposes certain provisions to facilitate interoperability of data, data sharing mechanisms and services. Ecommerce Europe generally supports the creation of consistent standards, but it is important that policymakers clarify the definition of "service type", 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. In addition, we ask policymakers to clarify the concept of "operators of data spaces" and the entities that fall under this category.

The prescriptive contractual requirements in Articles 23 and 24 also go beyond what is reasonable and common legal practice in a B2B (and even B2C) context. Some of these requirements would also likely lead to cost increases for the user. Article 23 (1) (a) lays out a 30-day termination period which, along with a prohibition on switching charges (Article 25), would eliminate the ability of EU businesses to negotiate price reductions in exchange for longer term (multi-year) contracts. No possibility is provided for data

processing services to recuperate such costs, yet this should be considered and addressed in the proposal. The introduction of such mandatory 30-day termination periods would limit the providers' freedom of contract, which is protected under Article 16 of the Charter of Fundamental Rights of the EU and it would in practice give sophisticated business customers of cloud services greater rights than individual consumers have under applicable EU consumer laws.

7. International Data Transfers

Article 27 of the Data Act proposal introduces technical, legal and organisational measures to prevent international transfer or government access to non-personal data held in the EU where such transfer or access would conflict with EU or Member State law. Ecommerce Europe is concerned that this article could have negative consequences on businesses' ability to transfer data internationally. The article states that any request from a third country authority to a provider of data processing services to transfer from or give access to non-personal data within the scope of this Regulation would have to be based on an international agreement (Article 27.2). The ambiguous language in the provision could likely lead to problematic and diverging interpretations resulting in localization requirements that arguably would be inconsistent with other EU rules and commitments (e.g., Regulation on the Free Flow of Data, WTO commitments, etc.). We call on policymakers to clarify which international agreements are referred to in this article. When drawing a parallel to the experience of international data transfers under the GDPR, in which many (small) businesses are at risk of severe damage to their business due to legal uncertainty, we strongly urge policymakers to leave no doubts about the scope of this article and about the type of data that would be covered. Finally, from a user perspective, this chapter risks restricting the free choice of cloud services in Europe, increasing red tape and costs for both service providers and users and potentially even undermining international competitiveness of European industry. We believe that if any, that it should be the European Commission to list 3rd countries that are not adequate to EU standards. Putting instead this burden on individual data processing service provides risks leading to significant uncertainty in the markets.

8. Enforcement

The Data Act proposal makes Member States responsible for the implementation and enforcement. They will have to establish new competent authorities in charge of the enforcement at national level, but also maintain the responsibilities of Data Protection Authorities with regards to personal data. Ecommerce Europe is cautious that such a fragmented approach to enforcement could also lead to regulatory fragmentation within the EU, which could result in legal uncertainty for businesses and potential barriers to operating cross-border. We urge policymakers to explore how enforcement could be more harmonised to ensure a consistent implementation across the Union. Finally, Ecommerce Europe calls on the Commission to issue timely guidance documents to facilitate implementation and allow for sufficient time for businesses to comply with the new rules.