EuroCommerce for retail & wholesale

*Position paper*
*13 May 2022*

# Proposal for a Data Act: Promote measures for an innovative data economy

***Key points***

- EuroCommerce supports the aim of the European Commission to encourage further access and use of data in order to mutually benefit public and private actors. **Voluntary contract terms**, with the involvement of industry actors are welcomed **especially for SMEs which often lack the resources.**
- Businesses need **clear rules and legal certainty especially in an area such as data,** therefore we would **welcome clarifications on the scope** and many **definitions (data, product, related services)** covered by the proposal.
- **Government access to private sector data** needs to be subject to EU-level rules and safeguards to avoid regulatory fragmentation and needs to strictly define the data and the purpose of such access. Repeating an effort of establishing a mechanism that resembles to the proposal for a **Single Market Information Tool (SMIT)** which lapsed during the last parliamentary mandate should be avoided.
- The Commission should propose stronger and **concrete safeguards for trade secrets** to create a framework for companies to feel safe in sharing more data which is also in compliance with competition rules.
- Some provisions will **undermine companies' contractual freedom** and discourage data use and sharing, have the opposite effect to that intended. Contractual data-sharing agreements should remain voluntary and respect competition rules.
- The measure should provide **incentives for companies to share data** and avoid creating mandatory obligations that risk discouraging investment in high-value datasets or risks undermining the use of such high-value datasets by ancillary service providers/consultancies.
- **Businesses need clarity on the use of data generated by connected devices**, including how to access and share it.
- In most cases datasets collected by connected devices **can be mixed (personal and non-personal data)** and it is important that any data sharing would remain in line with **GDPR** and privacy laws.
- The current proposal risks overriding the provisions of the **GDPR governing international data transfers**, creating serious obstacles for the normal data requirements of many EU businesses.

# Introduction

The Data Economy and its insights can help retailers and wholesalers to improve services, foster digital and green innovation. Providing replies and opportunities to the long-standing issues of data access and interoperability within safe and easily accessible data environments is very important for public bodies, companies, and individuals. The retail and wholesale sector already shares data with public authorities to fulfil regulatory obligations (e.g. traceability, registration of chemical substances, statistics) or requests from governments (e.g. for statistics, tax, or other purposes). We recognise the value of sharing certain data with public sector bodies to serve the public interest. **In particular during the covid crisis retail businesses clearly showed that they are willing to offer data to public authorities and governments in order to assist in implementing social distancing and other related measures that were imposed due to the health crisis.**

We support the aim of the European Commission to encourage further access and use of data in order to mutually benefit public and private actors. However, as common practice already shows, data sharing and data access can only be successful if it remains voluntary, i.e. if companies can decide for themselves which data they want to share or grant access to, when and to whom. A voluntary approach would support data reuse while safeguarding the competitiveness of European businesses, helping companies grow and securing adequate investment for data management. In that direction the Commission proposals on voluntary model contract terms are welcome**,** especially for smaller companies, that often lack the necessary legal resources and capacity to negotiate contractual data sharing agreements and are often in a weaker bargaining position. We welcome also that the Commission will involve industry actors in the drafting of these models. However, some of the provisions of the proposal encroach too far on entrepreneurial freedom do not provide the necessary safeguards for businesses to share data. Above all, new rules on data sharing should be pragmatic, based on what is technically feasible and economically viable, and consistent with overlapping legislation, in particular the General Data Protection Regulation and competition rules. Please find below our more detailed comments on specific provisions.

# Scope/Definitions – more clarity is needed

## *Scope*

The **scope of the proposal is too broad** and its one-size-fits-all approach creates a lack of clarity. According to Article 1, for example, the Data Act is intended to cover all sectors, without taking into account sector-specific differences in the data law. The right to data access cannot be an end in itself, and the positive intention of creating competition in one area can have unforeseen (negative) consequences for competition in other sectors. Broad horizontal rules covering all sectors risks overburdening businesses in sectors where no problems have been identified and where well-functioning contractual arrangements are in place. Nevertheless, we observe that the current scope will include more areas than it was originally intended by the Commission. EuroCommerce understands that the primary aim of the proposal was the IoT data and that we believe that it should stay within the IoT, as to avoid more players falling under the scope while that was not the intention of the proposal. Scope should be keep to the preliminary aim. Concrete gaps identified in specific sectors (e.g. car repairs, insurances) could be handled better with separate initiatives that are already in the process of being drafted.

## *Definitions*

The proposal remains unclear as to whom the provisions will actually apply and which kind of data is affected. **The definition of data is very broad and unclear**. It is not clear what type of data is involved and how certain data, for example user-generated and product-generated data, are to be distinguished from one another. The first part of the proposal provides users with the right to access to and sharing of **IoT data** generated by connected devices. This contrasts with provisions on **business to government data** and the chapter on **international data transfer** and access where all types of business data appear to fall under the scope of the proposal. We are also very concerned regarding the definition of **product** within the proposal which is very broad and could cover many products and services, like payments methods that were not supposed to be included under the scope. We note that the definition used in the preliminary report of the **European Commission on the sector inquiry on IoT**[1] was more suitable in this context. **We would urge the Commission to adapt the definition in this direction.**

The definition of '**related services**' is also very unclear as it fails to delineate responsibilities between stakeholders in the supply chain and focus on those best placed to give access to data. Due to that more services and products will fall under the scope than it was originally intended originally.

It will be important to create clear definitions so that is clear in each case which economic operator is **responsible to share** this data and with whom. **In many scenarios, retailers could be considered as data holders and/or users**.

In most cases **datasets collected by connected devices can be mixed** (personal and non-personal data) and it is important that any data sharing would remain in line with **GDPR** and privacy laws. However, data holders according to the Data Act and data controllers according to GDPR are not necessarily the same entity, which raises questions as user access. In addition, it is immediately clear who will be the beneficiary of the enhanced right to port data "according to the concept of 'user' adopted by the Proposal. Individuals could become entitled to have access to the data only incidentally, depending on the legal title under which they use the product or the related service (ownership, rental or lease) rather than on their relationship with the information concerning their private use of the product or service.

Lastly, there should also be a **clear distinction between non-processed and processed data** and of what constitutes data aggregated by IoT or data aggregated by the data holder. The proposal is intended to cover only raw data. Data is a product like any other; it requires an investment of time and skills and incurs costs to become a valuable product and thus is covered by the sui generis of the Database Directive.

**We call on the Commission to clarify the definitions of the proposal and the types of data and devices falling under it to give businesses clarity in complying with the new rules. We also call on the Commission to add in the definition of users ''and the data subjects'' and clearly differentiate**

---

***"consumer IoTs related products and services"*** *is to be understood as products and services used by consumers that are connected to a network and can be controlled at a distance (COMMISSION DECISION - initiating an inquiry into the sector for consumer Internet of Things related products and services pursuant to Article 17 of Council Regulation (EC) No 1/2003. 2020)*

**the situations where the user is the data subject from the situation where the user is not the data subject to ensure compliance with the GDPR.**

## Provide more clarity regarding B2B and B2C data sharing

We welcome the Act's intention to promote data sharing through new obligations for the B2B access to user-generated data for entrepreneurs. This can allow companies to save costs, gain new insights, develop new business models, etc. However, the basis of B2B data sharing **should fundamentally be an agreement between the respective parties, based on the principle of freedom of contract and in respect of the rights of the data owner to control what purposes that data can be used for**.

We welcome the consumer-focused objective of the Act, but requirements and regulatory burdens in B2C data sharing will have a negative impact, and the Act should adopt different approaches in B2B and B2C data sharing to avoid creating legal uncertainty for business. This right of access to data is too broad in its current form: it may have negative consequences for competition in some sectors. If the EU is to remain globally competitive and innovative, it needs a legally secure, efficient and automated framework for data exchange. In order to ensure this, safeguarding trade secrets and protecting existing business models is an important point that will actually help the aim of the Act in unleashing the potential of the European data economy.

### *Need of stronger protection of trade secrets*

The Act gives insufficient clarity on who has access to the data and what they are allowed to do with it, and how to guarantee the protection of trade secrets and shared or sold data. It is also unclear who will be liable for the protection of the shared or processed data, and which entity/actor will guarantee that the shared data does not fall into the wrong hands or is used for a different purpose than the one defined. The provisions of Articles 4 and 5 prohibiting companies from developing competing products based on data and the protection of trade secrets especially with regard to the protection of algorithms and innovations look very hard to enforce especially since business confidential data do not enjoy legal protection under this regulation. We wonder how the data holder can make sure that the user has actually taken all "specific necessary measures to preserve the confidentiality of the trade secret" and businesses can be ensured that their commercial interests are adequately protected. Also what is to be covered by these measures, or even what must be covered, is also not elaborated or defined in the proposal. Finally, extending the non-compete protection only to products but not to services themselves raises serious concerns. The service component of integrated solutions continues to grow in significance and increasingly represents the primary income stream. This is pre-programmed to create a major volume of litigation and uncertainty. It would also be necessary to clarify who exactly can gain access to the data as a so-called third party. This is not sufficiently regulated in the present case, as the term "third party" could theoretically include a large number of legal and natural persons. **The Commission should propose stronger and concrete safeguards for trade secrets and intellectual property rights to create a framework for companies to feel safe in sharing more data. In addition specific thresholds should be established in order to reach the right balance between any kind of obligation to disclosure detailed and commercially sensitive information and the need to provide users with an adequate level of data.**

### *Safeguard entrepreneurial freedom*

The draft Data Act contains approaches that can create important barriers to **entrepreneurial freedom.** The basis of a B2B data exchange should fundamentally be an agreement between the respective parties, based on the principle of freedom of contract. Data access and information obligations, restrictions on contractual freedom, requirements for technical design should only be justified if the market would be distorted without these measures. In the retail and wholesale sector we do not have any evidence of such market failures or gaps which are not being handled by competition rules. Past practice and experience have shown that the parties involved can reach a negotiated result that is fair and commercially acceptable for all sides under contractual freedom. The proposed provisions mentioned above are therefore **neither necessary nor helpful for our sector**. We fear that introducing user-centric one-size-fits-all rules that are in parts modelled after GDPR provision (e.g. disclosure requirements, purpose limitations) may in fact erect hurdles for more data-based innovation and interfere too much with well-functioning data relationships rather than facilitating sharing and use.

### *Implementation of data sharing should be taken into account*

If businesses are mandated to participate in an exchange of information by law, it is necessary for them to establish a flow of information that is usually located between different companies, i.e. different organisations, and different parts of an organisation. These requests entail businesses to include information in their internal structures which they do not want to have. Where information is exchanged, internal controls and firewalls need to be established to keep such information exchange in line with competition rules and requirements. Where the legal obligation to exchange information is not limited to what is necessary, it can create a disproportionate burden for businesses and potential liability under competition rules. **If legislation or administrative practices do not take these practical consequences into account or do not create adequate safeguards, particularly for the most sensitive procedures, it will fall to businesses to take the risk and compensate for the deficiencies or lack of consideration of this aspect.**

## B2G data sharing requires more clarity and safeguards

The **Data Act should encourage voluntary partnerships and refrain from introducing mandatory business-to-government data-sharing provisions which public authorities, (not least in countries where the rule of law is not very robust) could abuse.** We should avoid repeating an effort of establishing a mechanism that resembles to the proposal for **a Single Market Information Tool (SMIT)** which was lapsed during the last parliamentary mandate.

**B2G data sharing requests should be strictly limited to predefined data sets, should apply concrete conditions for use and for what purpose**, including remuneration and/or covering reasonable expenses. They should be directed at companies which have effective control over data**,** subject to a predictable and independent vetting process, as well as appropriate and clear safeguards such as purpose limitation, clear retention policies, as well as technical measures to protect data integrity, privacy, data protection and security. **Our opinion is aligned with the opinion provided jointly by the European Data Protection Board and the European Data Protection Supervisor**, where we read that access to data by public authorities should always be properly defined and limited to what is strictly necessary and proportionate, and suggest that lawmakers should define “much more stringently”

what is meant by exceptional need. The legislator should also clarify to which degree third party data that is stored by a company that receives a request, should be informed or have a say in the sharing process. Suppliers, business partners or customers may otherwise have their data unwittingly disclosed without proper process rights.

According to Article 14 a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested. **In this context, an exceptional need according to this text may not only exist if the requested data are necessary to respond to a public emergency** or if the requested data are limited in time and scope and are necessary to prevent or assist in dealing with a public emergency. Rather, according to Art. 15 (c), **this need may already exist if the lack of available data prevents the aforementioned entities from performing a specific task in the public interest** that is expressly provided for by law and they were unable to obtain the data by other means. Although the exception created here for small and medium-sized enterprises is to be welcomed, this right of access for public bodies is very broad. The conditions described here for an exceptional need are too vague. Furthermore, the Commission should take under consideration that many companies are already following very extensive obligations, so duplication of obligations should be avoided as the would lead to legal uncertainty.

**A large number of situations could be defined under it that have nothing to do with a public emergency. As a result, the thresholds for public sector bodies to access data are very low and are far from limited to emergency situations. Such a broad obligation to share data is disproportionate and without the necessary safeguards in place it could end up exposing commercially and privacy sensitive data.**

Lastly, in terms of safeguards against potential exposure of commercially sensitive data it is worth noting that last year, public administrations suffered from more security incidents than ever before. **More clarity is needed around accountability and potential penalties in the proposal for any misuse of data**.

## Clarify data access and fair conditions

The Data Act **lays down the horizontal foundations for sector-specific initiatives** based on the principles of fairness, transparency, proportionality, reasonableness, and non-discrimination. Nevertheless, fairness is very difficult to define in a legal text and subject to subjective and differing interpretation at the EU and national level leading to legal uncertainty, possible litigation, loss of agility and overall reluctance to share data. Differences in negotiating power are unavoidable and are present everywhere in the economy. The proposal risks an overburdensome obligation on the data holder to prove that the conditions for making data available are non-discriminatory, whenever an enterprise “considers” the conditions to be discriminatory while providing and unsatisfactorily open list of what can be defined as ‘unfair’. **Businesses need clear rules and legal certainty especially in an area such as data management where a lot of investment has been made and will continue to be necessary.**

### *Ensure policy coherence*

Current provisions in competition law for information exchange work well and further guidance on horizontal and vertical agreements is being considered as part of the ongoing review of EU

competition rules. Some issues relating to access to data in digital markets where a business is judged to be a 'gatekeeper' are addressed by the Digital Markets Act. We note in this that while policy coherence with the final text of the **DMA** is important, we are not convinced that the term gatekeeper is fit for purpose in the Data Act and further discussion and clarification are needed. In addition, as the process of sharing non-personal data is very different to the processing covered in the **GDPR**, further guidance on the interrelation between the two laws and other relevant rules as the **AI Act** would be required. GDPR is the blueprint for all further digital and data-related legislative proposals therefore any disclosure of personal data must follow the legal basis under data protection law for a data transfer in the sense of Art. 6 and Art. 14 of the GDPR. Lastly, the Data Act should also be coherent with the ongoing discussion on the creation of the **Digital Product passport in the Sustainable Product Initiative proposal**.

## Create incentives fostering data sharing

Incentives, rather than obligations, would encourage companies to further share data in a responsible and safe manner without jeopardising trade secrets or the competitive advantage of a well-functioning business model. Incentives for data sharing range from business strategies for testing innovation opportunities around the core business models or directly monetising data (e.g. in selling data sets to businesses or governments for specific applications), or as part of the value proposition and basic provision of the service (e.g. access to raw and aggregated data of the platform by business users of online marketplaces). Some companies are also incentivised to share data for public interest considerations (e.g. in sharing data with charities, public bodies or researchers).

Incentives for companies to share data should not be undermined, particularly where it could discourage the third-party providers from continuing their services (e.g. less profitable). This may be particularly important for medium-sized or mid-cap enterprises, that are large enough to need these services, but which lack the in-house expertise.

The Data Act **should build on existing data sharing best practice** to lay down the conditions under which companies may voluntarily share data with other businesses. It is crucial that companies retain the freedom to choose the governance model and technology that suits them best. The Act can provide practical tools for companies interested in making their data available and/or accessing data from others. The voluntary model contracts already included in the Data Act are a welcome step in this direction and others might be provided, building upon relevant EU legislation including data protection and privacy, security, intellectual property rights, database rights, trade secrets.

Lastly, the Data Act should include **ethical guidelines on the use of data,** including for the public interest, and, where relevant, taking into account the ethical AI guidelines. Companies should be ensured that their data is stored and shared in an ethical, cybersecure manner always respecting competition rules. This would create a more holistic approach towards promoting more data sharing in the coming years.

## Interoperability should be based on existing data sharing systems

The proposal lays down requirements to facilitate interoperability of data, data sharing mechanisms and services. It is essential that systems already in place which facilitate data sharing, particularly automated data sharing, should be taken into account. The Data Act should not oblige businesses to

adapt their existing systems in order to enable interoperability. This would lead to additional and unnecessary costs, depending on the nature of the data and perhaps the cybersecurity features put in place. In addition, we would call on the Commission to clarify the term “operators of data spaces” and the entities that fall under this category.

## Clarify unclear provisions international access and transfers

The Data Act 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 contravene EU or Member State law. Third-country requests for access or data transfer will only be considered valid if based on an international agreement between the requesting country and the EU or Member State. We would welcome clarification from the Commission to which international agreements they are referring or whether any of these are being negotiated with major EU trading partners. At the moment third country adequacy decisions and agreements such as the recently announced agreement between the EU and the US, along with the existing standard contractual agreements and supplementary measures are in place to ensure the safe transfer of personal data. Would similar arrangements be proposed for non-personal data? The Data Act should not risk erecting a barrier for international data flows or leading to data localisation requirements, without even a prior judicial assessment. It should not restrict the choice of technology and the EU’s capacity for innovation and should avoid limiting the ability for EU businesses to grow and compete internationally. While in the case of personal data consumers should enjoy additional protection afforded by the GDPR, companies that have the capacity to weigh the risks, if any, of using specific providers should be free to do so as it concerns their own data. **We call on the Commission to clarify what type of data are covered by the scope of this article of the Act.**

## Switching data processing services is complex

We are in favour of the principle of data exchange to facilitate cloud switching options and to promote competition by removing blockers for cloud customers. However, the suggestion in the proposal that cloud switching is similar to a relatively straightforward migration of stored data or to free-of-charge portability operations under the GDPR does not reflect the reality of many cloud services. The volume and complexity of data, the shared responsibilities between cloud providers and customers and the need for specialist technical assistance and project management make this a much more difficult process. Compatibility between receiving and sending services can only be achieved by both services cooperating in offering this. Switching between a wide variety of incompatible providers makes this obligation impossible to achieve comprehensively and smoothly. Any such requirement cannot simply be imposed on the companies involved, and can only work if the EU and member states establish the necessary set of standards and standardisation offerings to allow such switching to work.

The obligation of "maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type" simply does not work. It risks being be a massive removal of contractual freedom and blocking innovative product design, hindering competition and innovation in Europe and involve significant costs. These switching obligations appear to overlap with the portability obligations under DMA. **DMA obligations applicable to cloud computing providers should be clarified further under the Data Act and the obligations mush be aligned to avoid duplication.**

## Risk of fragmented and ineffective enforcement

Enforcement of the Act is split between different regulators and left to individual Member States. The proposal allows each country the discretion to enforce the rules differently. This approach will inevitably lead to a fragmented approach across the EU, with major additional burdens for companies operating cross-border. This is not likely to help create a uniform and globally competitive EU data market. This **requires a more harmonised approach and consistent implementation of the Data Act and close monitoring and cooperation between the relevant authorities.**

The Data Act also makes a reference to article 33 of the GDPR proposing fines up to 4% of turnover. We support clear rules and proper enforcement. But, as many data protection authorities have concluded, high fines on entities are not the most effective way to ensure compliance. **We support a more collaborative approach to compliance, creating incentives for companies to share more data and for authorities to offer their assistance to ensure compliance when needed.** It is, we believe, inappropriate to propose such high fines for misuse of non-personal data with no reference to their proportionality to the likely damage arising. We would also welcome guidelines from the Commission and flexible deadlines processes and requirements. Businesses would need the appropriate amount of time to comply with the new obligations.

Contact:
Savvina Papadaki - +32 045 35 6163 - papadaki@eurocommerce.eu **Transparency Register ID: 84973761187-60**