Independent Retail Europe

EU DATA ACT

- POSITION PAPER OF INDEPENDENT RETAIL EUROPE -

12 September 2022

Avenue des Gaulois 3 / box 3
B – 1040 Brussels

T + 32 2 732 46 60 F + 32 2 735 86 23
@ info@independentretaileurope.eu

www.independentretaileurope.eu
Transparency Register : ID number 034546859-02

COMMENTS OF INDEPENDENT RETAIL EUROPE ON THE EU DATA ACT

Independent Retail Europe welcomes the EU Data Act's aim to maximise the value of data by ensuring that more data is available for innovative use. This will allow retailers to develop new services on the aftersales market. However, we have major reservations about the interplay between the EU Data Act and various other EU legislation and about the lack of sufficient safeguards to protect trade secrets, while Chapter V raises important questions about its compatibility with the EU legal order.

Main aspects covered in this position

Issues related to the scope and definitions:

- Align the definition of data on the internationally accepted definition under ISO standards;
- Align the definition of 'product and services' with the definition used in the IoT EU sector's inquiry;
- Clarify the interplay between the EU Data Act and the GDPR/Data Governance Act;

Protection of trade secrets and risks of conflict with EU competition law:

- Data sharing obligations should not apply to data processed by the data holder unless they relate to essential data for the functioning/repairing/servicing of IoT products;
- Introduce legal safeguards in line with EU competition law for cases where data sharing obligations may lead to share 'commercially sensitive' data with competitors;
- Provide a more explicit obligation to put in place structural measures when sharing data that contain trade secrets or commercially sensitive information (as defined under competition law);

Pre-contractual information on smart products:

- Amend article 3(2) to ensure that product manufacturers are responsible for providing the required pre-contractual information to the final user by making it accessible on the package;

Unfair B2B data sharing contract terms:

- Do not extend the list of unfair B2B data sharing contract terms, as this would disincentivise voluntary data sharing partnerships;
- Align standard contractual clauses for the sharing of non-personal data on standard contractual clauses for the sharing of personal data;

Mandatory B2G data sharing obligations:

- Chapter V raises major concerns over its compliance with key principles of the EU legal order due to the vagueness of various concepts and of the hypotheses for the use of article 15 – as reported by the European Data Protection Board joint opinion on the Data Act;
- The precedent of the (withdrawn) Single Market Information Tool (SMIT) raises major doubt about the lawfulness of the legal basis proposed (art. 114 TFEU) and about the compatibility of broad B2G data sharing obligations with the EU Charter of Fundamental Rights. The Council and European Parliament's legal services should request an opinion on the lawfulness of article 15-c in light of the SMIT precedent;

- ➔ Article 15-c could be used by public services operated by public bodies to unfairly compete with private companies operating a competing service – therefore breaching competition law.
- ➔ The use of Article 15-c by public bodies to address data sharing requests to companies that do not operate in the same Member States would lead to disproportionate burdens and a potential unlimited number of data request.
- ➔ In light of the above issue, article 15-c should be deleted.

1. The scope and key definitions need to be more precise

While we welcome the overall aim of the EU Data Act, we consider that the scope of the proposal and certain key definitions are too vague. As a result, it is currently unclear whether and, if so, how, the EU Data Act will apply to the retail sector in a wide range of situations. Such a situation would increase the regulatory burden and risks of non-compliance. Legal instruments should be clearly defined when they impose obligations subject to sanctions.

a) The definition of data should be based on existing internationally accepted definitions

The proposed definition of data (art. 2(1)) is rather vague. Moreover, it does not correspond to other internationally accepted definitions of data, notably the one defined in international standardisation processes. This leads to important legal uncertainty.

The definition of data in article 2(1) should therefore be clarified and based on internationally accepted definitions, such as those referred in ISO standards 9000:2015 and 9001:2015, which clearly define the terms 'data' and 'information'.

b) The definition of 'products' and 'related services' should be aligned with the definition used in the EU sector inquiry on IoT

While we welcome the goal and most of the provisions in Chapter II and III, we believe that the definition of products and related services subject to these chapters is too broad/vague. This will lead to legal uncertainty.

We believe that the EU Data Act should instead use the definitions used in the preliminary report of the European Commission sector inquiry on IoT[1], as these are clearer, have already been tested in practice, while using them would avoid any unintended/unassessed expansion of the scope of the Data Act in the future.

c) The definition of 'products' and 'related services' should exclude payment instruments covered by the PSD2

1 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)

Although the EU Data Act is not supposed to affect other sectoral EU legislation[2], the definition of 'products' and 'related services' would in practice cover electronic payments (e.g. card transactions, mobile transactions, e-vouchers) normally regulated by the Payment Services Directive 2 (PSD2).

To avoid any conflict of law, or any unintended application of the EU Data Act to payment instruments regulated by the PSD 2, **the EU Data Act shall make clear that its definition of 'products' and 'related services' does not apply to such payment products or services covered by the PSD2.** Alternatively, article 1 of the EU data act should clarify that it does not apply to products regulated by the PSD2.

d) The interplay with the GDPR, the Data Governance Act and EU competition law should be clarified

It is unclear how the EU Data act will interplay with other EU legislation such as the GDPR and the Data Governance Act. The recent opinion of the European Data Protection Board on the EU Data Act points to a lack of clarity which may lead to legal uncertainty on the applicable framework in specific situations. Clarifications are needed.

Moreover, it is also unclear how the EU Data Act will interplay with EU competition law, and may even in some cases contradict it in practice – see section 2 below.

Key recommendations on the scope, definitions and interplay with other EU legislation:

- **Align the definition of data used in article 2(1) on internationally accepted definitions used in ISO standards 9000:2015 and 9001:2015**
- **Align the definition of IoT 'products" and 'related services' on the definition used in the preliminary report of the European Commission sector inquiry on the IoT;**
- **Clarify that the EU Data Act, or at least the definition of 'product' and 'related services' does not apply to products and services regulated by the PSD 2.**
- **Introduce clarifications on the interplay between the EU Data Act and the GDPR and the Data Governance Act.**

2. Stronger safeguards to protect trade secrets and avoid conflicts with EU competition law

Overall, we support the objective of the Data Act to open up the aftersales market of IoT products and services. This market is currently subject to a lack of competition, as highlighted by the recent EU sector inquiry on the IoT. We therefore support the ambition of Chapters II and III, as they will allow for the emergence of new service providers that will provide new innovative services to consumers, based on IoT data (e.g. retailers to develop innovative aftersales services for smart products sold in their shops).

However, the EU Data Act foresees insufficient safeguards to protect trade secrets from being accessed to by third-party competitors. Moreover, additional safeguards are needed to avoid conflicts with EU competition law when the EU Data Act may lead to exchange commercially sensitive information with competitors.

---

2 See page 5 of the Commission's explanatory memorandum COM(2022) 68 final: *"[…] the rights and obligations on data access and use have also been regulated to varying degrees at sectoral level. The Data Act will not change any such existing legislation […]"*

a) Data processed by data holders and unrelated to the functioning of an IoT product should not fall into the scope of the Data Act

The EU Data Act fails to distinguish between "raw data" and "processed data" or between data aggregated/processed by an IOT product or related services and data aggregated/processed by the data holder. As a result, it is unclear how trade secrets can be preserved. Raw data are of little commercial value in itself, while processed data require extensive investments (financially, technically and in terms of human resources) and represent an extremely commercially sensitive asset for any company that will determine its ability to compete on the market.

It should be absolutely clear that data processed/aggregated by the data holder which are not related to the functioning of an IoT product or related service do not fall into the scope of the EU Data Act, as this would otherwise create major obstacles to investments in data and innovation (resulting from the weakening of trade secrets protection). On the other hand, it is crucial that users and data recipients may have access to data which are essential to the functioning/repairing/servicing of an IoT product.

Therefore, article 1 should clarify that the Regulation shall not apply to data processed by data holders unless such data is essential to the functioning/repairing/servicing of IoT products and related services. Article 2 should include a definition of processed' data for this purpose. Processed data not related to the functioning/repairing/servicing of a product should be considered as a protected trade secret not subject to mandatory divulgation/sharing.

b) Stronger safeguards should be introduced to preserve trade secrets and avoid misuse of data by competitors

Article 4(3) and 5(8) of the proposed EU Data Act intend to protect trade secrets from data holders by minimising risks of their divulgation that may arise from the mandatory sharing of IoT data, and by establishing a prohibition to use the data shared to develop competing IoT products.

Unfortunately, these articles provide an insufficient level of protection of data holders:

- Article 4(3) and 5(8) are too vague as to the protection that shall be put in place to prevent data holders' trade secrets from being used by the user/third parties. In addition, the failure to distinguish between raw and processed data subject to the sharing obligations (see above) raises a major risk of sharing trade secrets and commercially sensitive data.
- The prohibition contained in these articles to use data to develop a competing product or service will be extremely difficult to monitor/enforce in practice. This may raise a global risk of widespread abuse and litigation.

It is therefore *extremely important* to strengthen the safeguards foreseen in Art 4(3) and 5(8) of the EU Data Act to effectively protect trade secrets. A provision should be introduced to explicitly acknowledge data holders' right to put into place structural measures to prevent trade secrets from being accessed and used by third parties.

c) The EU Data Act should not conflict with EU competition law

The recent draft revised Horizontal Guidelines (published for consultation by the European Commission) contain specific guidance on data sharing required by law, which would therefore be applicable in the context of the EU Data Act B2B data sharing obligations involving competitors.

This draft guidance specifies[3] that in such a case, EU competition law still applies in its full strength, and that specific measures must be put in place to minimise competition risks, including possible restrictions on the scale and frequency of data exchanges.

Given the broad definition of data, and the extent of data sharing obligations foreseen in the EU Data Act**, a direct conflict with competition law is likely to arise in cases where data holders will be obliged to share commercially sensitive data with competing third parties**. This may concern both, B2B data sharing obligations (e.g. mandatory sharing of data generated by IoT) but also possibly B2G data sharing under article 15-c (when a public body offers a public service in competition with a business to which it addressed a data sharing request – see section 5 of this position). **The EU Data Act currently does not include legal safeguards to prevent potential conflicts with EU competition law obligations.**

Key recommendations:

- **Support the objective to open up aftersales markets of IoT products, as broadly proposed by Chapters II and III;**
- **Clarify that the EU Data Act data sharing obligations do not apply to processed data (which are strategic assets /trade secrets) unless related to the functioning/servicing/repairing of an IoT product/related services;**
- **Introduce legal safeguards in line with EU competition law to cases where the data sharing obligations foreseen by the Data Act may lead companies to be obliged to share 'commercially sensitive' data (as defined under EU competition law) with competing third parties;**
- **To prevent possible abuse of the data to unfairly compete with the data holders, introduce an obligation to put in place structural measures when sharing data that contains trade secrets or commercially sensitive information (as defined under EU competition law). E.g. Chinese walls, strict access protocols with restricted access rights, non-disclosure agreements, etc.**

3) The obligation to provide pre-contractual information for smart products is unpractical if not included on the package of the product

Article 3(2) requires the provision of some minimum pre-contractual information for the purchase, lease or rent of a product or related service covered by the EU Data Act in B2B and B2C settings.

However, neither this article nor corresponding recital 23 clarify who should be responsible for this pre-contractual information. Moreover, article 3(2) only requires the provision of mandatory information towards the user of the smart product or service, whereas most smart products will not be sold to final users by the manufacturers, but mostly by distributors, who may have purchased the product from either another distributor - a wholesaler or an importer - or the product manufacturer.

The pre-contractual information obligation foreseen in article 3(2) cannot work in practice if the manufacturer does not first provide the information to the next entity in the supply chain (i.e. a wholesaler, an importer, or a distributor), who then have to transmit the information to the next entity in the supply chain, etc. until it reaches the final user.

3 See in particular para 411 of the draft revised Horizontal Guidelines

In addition, most retailers selling smart products covered by the EU Data Act will lack the necessary technical knowledge about the product to be able to easily inform consumers verbally about the aspects mentioned in article 3(2), and cannot store in their own warehouses the necessary documentation (due to limited storage space available and the rapidly increasing number of smart products being sold by retailers); Nor will every consumer be able to ask verbally the staff of the retail shop for the information at the pre-contractual stage.

Therefore, to be workable in practice, any pre-contractual information about smart products to be communicated to the user should be labelled on the package of the product, as such a pre-contractual obligation would be impossible to fulfil for retailers given the potential number of products concerned. Such a clarification would be consistent with the EU acquis on product legislation, where the manufacturer is always responsible for providing (either on the package or inside the package) the necessary product information to the final user.

Key recommendations:

- **Amend article 3(2) to ensure that product manufacturers and service providers are responsible for providing the pre-contractual information to the final user. In the case of products, manufacturers should ensure that the information is accessible on the package.**

4) Unfair B2B data sharing contract terms (Chapter IV)

First of all, we consider that best practices in data-sharing agreements and creating new voluntary and safe models to share data (such as will be done by Data Governance Act) will likely provide more incentives to share data than the proposed prohibition of unfair contract terms in B2B data sharing agreements.

We fear that an extensive list of prohibited contract terms in voluntary data-sharing agreements with SMEs is likely to lead to less data-sharing agreements with SMEs than otherwise would occur. Data that is essential to other companies will also be subject to EU/national competition law, including fair access terms when this may impact competition. We therefore urge the EU institutions to not extend the proposed list of unfair contract terms and to keep it as short as possible.

Moreover, the EU Data Act should provide that standard contractual clauses for the sharing of non-personal data should be aligned on standard contractual clauses for the sharing of personal data.

Key recommendations:

- **Do not extend further the scope and the list of unfair B2B data sharing contract terms, as this would dis-incentivise voluntary data sharing partnerships**
- **Align standard contractual clauses for the sharing of non-personal data on standard contractual clauses for the sharing of personal data.**

4) Mandatory B2G data sharing: stronger safeguards shall be introduced

Chapter V provides obligations for Business-to-Government (B2G) data sharing in two cases: Where the data is necessary to prevent/respond to a public emergency (art 15-a and 15-b), or where the lack of data prevents a public body from fulfilling a task of public interest provided by law (art 15-c).

Such broad obligations raise important issues: problems with legal certainty, proportionality and compliance with the EU legal order, a questionable legal basis, a risk of unfair competition in cases where public bodies are in competition with private companies, as well as issues surrounding the territorial scope of application of the B2G data sharing obligations.

Therefore, we consider that the new generic B2G data sharing obligation under article 15-c should be deleted. Chapter V should exclusively focus on B2G data sharing where data is necessary to prevent/respond to a public emergency (art 15-a and 15-b).

a) Risks for legal certainty and compliance with the EU legal order

The vagueness of the provisions on B2G data sharing obligations, and the lack of proper safeguards to preserve the fundamental rights of data subjects and data holders raise major concerns over legal certainty and the compatibility of Chapter V with the EU's legal order, the EU Charter of Fundamental Rights and the ECJ's jurisprudence.

In its recent opinion on the EU Data Act, the European Data Protection Board (EDPB) expresses its "*deep concerns on the lawfulness, necessity and proportionality of the obligation*" foreseen in Chapter V[4].

The opinion stresses the following problems, amongst many others:

- The relevant tasks of public interest and the public sector bodies tasked with a mission of public interest have not been identified by the proposal;
- The circumstances justifying access to the data have not been defined narrowly, raising concerns over their legality under the EU legal order, in particular their compatibility with the principle of necessity and proportionality, and with the need to provide "*sufficient safeguards to protect individuals against arbitrary interference*"[5];
- The first use case of article 15-c raises major concerns over the foreseeability of the interference with fundamental rights, while the second use case of art 15-c does not meet the legal requirement for the necessity of such interference[6];
- Categories of personal data that can be accessed are not sufficiently specified, while safeguards for data subjects are not sufficiently spelled out[7].

Moreover, the compatibility of the broad data sharing obligation foreseen in Chapter V with the Charter of Fundamental Rights, and in particular its article 17, is highly questionable. Indeed, we would like to point out the similarity of the B2G data sharing obligations under Chapter V with the Commission's proposal for a Single Market Information Tool. Such proposal had to be withdrawn after the Council acknowledged[8] the risk of incompatibility of mandatory information sharing provisions with the Charter of Fundamental Rights (and the lack of a valid legal base under EU law – see below).

4 See the EDPB-EDPS Joint Opinion 2/2022 of 4 May 2022, page 2 and pages 20-23.
5 See the EDPB joint opinion para 77 and CJEU case C-175/20.
6 See the EDPB joint opinion para 79
7 See the EDPB joint opinion para 80 and 81
8 See 'Non-paper on the European Commission's proposal for a Regulation on the Single Market Information Tool' submitted to the Council on 13 October 2017 - WK 11397/2017 INIT)

A new general compulsory B2G data sharing empowerment as foreseen by article 15-c (to fulfil a task provided by law) is very much like a general right of access to a company's private data. In the absence of any suspicion of a legal infringement, such a generic power inevitably raises major concerns as to its compatibility with the EU Charter of Fundamental Rights, and in particular its article 17 protecting the right to private property.

In its current scope, article 15-c therefore creates unforeseeable and disproportionate interferences with data holders' fundamental rights. This generic data sharing obligation under article 15-c should be withdrawn.

b) The legal basis of the Data Act may be incompatible with broad B2G data sharing obligations

As pointed out above, the type and scope of B2G data sharing obligations under Chapter V of the Data Act is very similar to the obligations foreseen under the – now withdrawn – proposal for an EU Single Market Information Tool (SMIT). Both legislative proposals are based on article 114 TFEU.

However, the Council rejected the SMIT because article 114 did not constitute a valid legal basis for a legislative proposal imposing **broad** B2G data sharing obligations (under similar conditions as in the Data Act). Indeed, Article 114 TFEU can only be used to approximate national laws with the view to establish the internal market, while the broad B2G data sharing obligations under the SMIT were not directly linked to any existing information requirements that would apply under the rules of the single market.

Given the strong similarities between the SMIT data sharing obligations and Chapter V of the EU Data Act, is doubtful that article 114 constitutes a valid legal basis for the broad B2G data sharing obligations foreseen by article 15-c. We invite the Council and European Parliament to request an opinion from their legal services as to the lawfulness of the legal basis proposed in light of this precedent.

c) Risk of unfair competition by public bodies in competition with private entities

Article 15-c provides for mandatory B2G data sharing with public bodies, in case the public body requesting it needs the data to fulfil a task of public interest provided by law.

In the absence of a narrow definition of 'public interest', this article could be used in cases where a public body provides a public service in competition (for the same service) with a private company, allowing this public body to extract sensitive information to unfairly compete with its private competitors. **This would represent a clear case of unfair competition and would entail major breaches of EU competition law.**

d) Territorial scope of Chapter V – case of cross-border requests

Chapter V of the EU Data Act does not clarify whether the provisions on mandatory B2G data sharing car be used by a public authority to impose data sharing on companies which are not based or do not operate in the territory of that authority.

The introduction by article 15-c of **the possibility for public bodies to address compulsory B2G data sharing requests across the EU (to companies that do not operate in the country where the public body is established) would be unworkable** given the number of public bodies/authorities that could use such possibility for an infinite number of issues.

At the same time, Member States do not need an EU legal act to introduce data sharing obligations on companies which operate in their territory.

Key recommendations on Chapter V:

- **Specify explicitly the categories of personal data that can be accessed, while excluding sharing of processed data (which are protected trade secrets);**
- **Given the precedent of the SMIT, the Council and European Parliament should request their legal services for an opinion on the compatibility of article 15-c with the legal basis proposed (article 114 TFEU) and the Charter of Fundamental Rights.**
- **In light of the legal doubts surrounding article 15-c, and given the issue this article raises for the application of competition law (in cases public bodies compete with private operators for the provision of some services) and for its (potential) disproportionate scope of territorial application, article 15-c should be deleted.**

Original version: English – Brussels, 12 September 2022