Association française des entreprises privées

Proposal for a Regulation on harmonized rules on fair access to and use of data (Data Act)
AFEP Position Paper

Member companies of AFEP (the French Association of Large Companies) support the objective of the Data Act to **stimulate innovation through better access to data from connected objects.** Considering principles favourable to fair data sharing is appreciated.

However, the companies regret the **absence of a detailed impact assessment** which could have specified the types of data already exchanged (or not) and allowed to **identify the market failures justifying this obligation to share data.**

This text thus raises questions regarding its scope, the definition of data and of the products covered. In addition, data having a cost (due to its creation, management, dissemination or preservation), it cannot be made available to users and third parties without filtering by the holder or compensation proportional to these costs. In addition, this text leads to putting into question the protection of intellectual property and business know-how in an eminently competitive world. Finally, it unduly increases their liability in a vague and vast legal environment.

A **clear definition of data** is therefore necessary. The conditions for sharing data must also be specified to preserve efficient business models while **stimulating innovation on competitive bases favourable to European economic players.**

Table of Content

Introduction

AFEP shares the Commission's objective of improving access to data from connected objects to support innovation, develop fairer markets, ensure greater interoperability and strengthen consumer and user confidence by requiring greater pre-contractual transparency.

Various provisions contribute to establishing principles that are favourable to fair data sharing (such as increased transparency on the data generated by the use of a connected object for both its user and third parties service providers, as well for the latter on the commercial conditions of access to this data, possibility for the product manufacturer to process data generated by the use of the connected object, etc.) and better harmonization of the market by encouraging the implementation of standard tools such as Application Programming Interface (APIs), smart contracts or common governance rules. For European players, the interoperability of cloud services could potentially lead to cloud services that comply with European values and rules.

This new legal framework requiring European companies to share their data however also poses real risks for them. It calls into question the principle of contractual freedom of economic actors, and this sharing can potentially go beyond the framework of the European Union. It also calls into question the protection of their intellectual property and their know-how in an eminently competitive world. It unduly increases their liability in a vague and vast legal environment.

Given these legal uncertainties and economic consequences, this text therefore requires clarification to circumscribe its scope and the risks for economic players if it wishes to achieve its objectives of supporting innovation while taking into account sectoral realities. Data is indeed information that has a cost of creation, exploitation, and therefore, dissemination. It can also be sensitive and expose European players and products to strong risks (see retro-engineering in particular). As a strategic and economic asset, it helps to strengthen European sovereignty.

It should be noted that this proposal is not based on a detailed impact assessment, which would have made it possible to specify, for example on a sectoral basis, the data that is already exchanged -or not. This exercise would have allowed to specifically identify market failures and their possible causes, before imposing a general principle of obligation to share (often for free) data.

In this context, a clear definition of data is necessary to then allow a better structuring of the provisions of this text (scope, obligation to share, responsibility of the actors, role of the public authorities, etc.). Similarly, appropriate protection of sensitive data must be ensured – the contractual solution proposed in the text appears insufficient.

Finally, while data sharing should be encouraged, unduly destabilizing existing innovation business models should be avoided, in particular due to free access to data. This text is in fact a source of competitive distortion insofar as it will fully apply to European players whereas it will only apply to foreign companies offering products in the Union, paving the way to a breach of fair competition conditions.

Although AFEP supports the horizontal approach sought by the European Commission in this proposal for a Regulation, it appears difficult at this stage to establish parameters and definitions adapted to very heterogeneous sectoral realities (e.g. on shareable data). However, a regulation that is too intrusive or poorly configured could quickly end up discouraging innovation in the Union. The horizontal approach could therefore be lightened and supplemented via sectoral acts capable of clarifying certain definitions and obligations in a more detailed and relevant manner, particularly in the context of European work on data spaces.

General remarks precede more specific comments on this proposed Regulation.

General remarks

The complexity of the text compared to other legislation

With the creation of new obligations, the Data Act impacts other horizontal legislation, in particular the GDPR.

Although the text indicates that the processing of data covered by the new Regulation must be carried out in accordance with the GDPR, their simultaneous application will prove difficult (see in this sense the opinion of the EDPB adopted on 4 May 2022). Thus, for example:

- the proposal introducing the idea of a principle of "sharing by design" (Article 3) is *a priori* in opposition to the "privacy by design" approach of the GDPR,
- the prohibition on using data received by a third party for profiling purposes (Article 6-2-b) appears contrary to Article 6 of the GDPR which defines the legal bases (processing made necessary for the execution of the contract, consent of the individual, public interest, compliance with a legal obligation or legitimate interest of the controller) allowing controllers to process personal data.
- while the GDPR obliges companies that collect personal data to guarantee its security throughout its life cycle, the Data Act encourages the data holder to share it continuously and in real time", thus raising the responsibility of the holder who can no longer ensure its protection throughout the value chain.

This confusion complicates the implementation of texts by companies and unnecessarily increases their efforts and investments to strengthen the data security and cybersecurity of their products.

The potential risk to European companies

This risk is reflected both in **strong challenges to the legal frameworks** structuring the European economy and in **additional administrative burdens** creating **distortions of competition** that are not conducive to innovation.

- The proposed Regulation assumes that data would already exist "off the shelf" and could be easily shared provided that the obligation to do so is introduced into law. Moreover, with data being readily available, free sharing would be the rule.

  Sectoral realities show, however, that this assumption is often wrong: in many situations, industrial companies are instead engaged in a continuous effort to extract, collect, format and process an increasing volume of data in order to make them usable. In these situations, developing innovation and data sharing can only be done by preserving the incentives for these manufacturers to continue to invest in increasing the general volume of data. Otherwise, the Regulation would have a counterproductive effect.

- **Respect for intellectual property rights and trade secrets** is essential in order to avoid distortions of competition for companies holding data and to maintain sufficient incentives for them to invest and innovate. The scope, which does not distinguish between EU users and non-EU users or third parties, could lead to weak protection of these rights and secrets, even with the safeguards offered.
- The text does not sufficiently consider -for example- the situations of obligation to share data that may contain **trade secrets with competitors** or companies that risk transmitting this information to competitors. The fragile safeguards envisaged (of a contractual nature, therefore insufficiently dissuasive and ex-ante controllable) are likely to slow down investments in innovation due to a lack of protection against potential breaches of business secrecy and distortions of competition. The proposal also leaves open the question of possible guarantees for the data holder if he does not succeed in reaching an agreement with the data recipients on the protection measures.

  In general, the data holder should be able to refuse this sharing, when these guarantees are not ensured or respected ex-ante, and this for exchanges with third-party users or public authorities.
- The exception introduced by the proposed Regulation (Article 35) to the Sui Generis right could jeopardize the **intellectual property of database producers**. The creation of databases indeed requires considerable human, technical and financial resources. This derogation could jeopardize their future investments, which would have a significant impact on the innovation capacity of European economic players.

- In addition, the fact that free sharing is established as a principle with few exceptions will constitute a strong brake on innovation in all situations where the data is not available "off the shelf" and where manufacturers must incur significant costs of extracting, collecting, formatting and processing data in order to make them usable. This could also lead to real distortions of competition with third countries.

  In this respect, preserving the incentive for industrial players to develop the volume of data available must be fully taken into account, as an essential condition for the further development of the sharing of this data.

Comments on the main provisions of the text

Unclear scope and definitions (Chapter I)

The concepts applicable to the Data Act must be clear, to ensure legal certainty for stakeholders and to harmonize possible interpretations within Member States. At this stage, the proposed definitions of data and related products or services that must be available are very broad, horizontal and sometimes not aligned with other existing texts (e.g Data Governance Act). The notion of a connected object not being itself defined, the data generated by a related product or service potentially covers a very wide field making future technological innovations insecure.

Data sharing and contractual frameworks also differ widely, depending on the economic sector or the type of activity considered (B2C and B2B). A differentiated approach would likely limit legal uncertainties and risks for businesses. Indeed, the obligation to share the data generated by the Internet of Things with users (consumers or companies) seems unlimited. However, these connected products generate a wide variety of data, differing in their volumes, natures or levels of processing, including depending on the sector. Possible market failures, incentives for innovation and the competitive situation within and outside the Union differ greatly depending on the situation considered.

As an example, the owner of the connected product and its user are poorly differentiated. It will be necessary for certain sectors to have to clarify the attribution of rights and obligations in situations where the configurations of use and ownership of the device are more complex than the manufacturer-user relationship.

It also seems difficult to determine whether the sharing obligation concerns raw data or consolidated data sets (data that have been processed, transformed or enhanced using a software process). At this stage, sectoral situations prevent an unequivocal position from being reached on the type of data that could be affected by a sharing obligation. As underlined above, while promoting data sharing is legitimate to a certain extent, it is also fundamental to preserve the incentive for players to invest in the development of data collection and processing upstream. This requires effective preservation of trade secrets or intellectual property rights and allow compensation for financial and human investments made by companies.

A clarification of what data and shareable data are within the meaning of the Data Act is essential and a priority to the structure of this text and its possible application. The difficulty lies in coming up with clear definitions capable of embracing the various sectoral realities, making it possible to intensify the sharing of data while preserving sufficient incentives to invest upstream and to maintain a global level playing field.

From there follow other improvements, in particular on many definitions such as those of connected object, user, third users, and exceptional needs / public emergency. Understanding the text will be easier in terms of data sharing or responsibility.

B2C and B2B data sharing obligations putting companies at risk (Chapters II, III and IV)

Articles on user's data access obligations are very detailed, often making them unsuitable for the multiplicity of cases and actors depending on the sectors and products. They do not sufficiently differentiate the specificities of deployment by companies of connected objects as part of their economic activities.

Ensuring appropriate principles at the horizontal level while leaving the details of sharing to sectoral acts and contractual agreements could help improve the understanding of this text and find the balance between preserving incentives to innovate, sharing data and maintaining fair competition.

In addition, while companies support the development of data portability (Articles 4 and 5 of the Data Act) in line with Article 20 of the GDPR, real-time portability nevertheless raises questions of technical implementation. Considerations are needed on whether it is indeed a constant sharing of data during the object's use or only at the request of the user, on an ad hoc basis.

This sharing also has unfair consequences for data holders:

- the majority of data sharing obligations do not allow for sufficient compensation, in the case of third-party access (or B2G sharing in cases of emergency). The technical costs of collection, formatting, processing and dissemination for the data holder should at least be borne by the third party or the public authority at the origin of the request for data sharing;
- if the data holder is required to make data available to the recipient under FRAND conditions (Article 8-1), it is still up to the holder to demonstrate the absence of discrimination when the data recipient considers the conditions of access to this data as discriminatory (Article 8-3);
- the "reasonable" nature of the compensation agreed upon between a holder and a recipient of data (Article 9-1) must be specified in order to better take into account the real value of this data and the cost of making it available, and national or European provisions likely to call into question this principle of compensation should be removed (Article 9-3);

Article 13 targets unfair contract terms imposed unilaterally on micro, small or medium-sized enterprises. This approach seems to be unsuitable in the digital world where any

structure can be economically powerful regardless of its size. As such, it is proposed to target "parties" instead of micro, small or medium-sized enterprises.

Mandatory provision of data to public services raising difficulties (Chapter V)

Here again, a detailed impact assessment would have been necessary in order to precisely identify beforehand the situations in which a market failure can be proven, justifying legislative intervention. Conversely, in many situations, data sharing with public authorities work satisfactorily and should not be destabilized. In particular, this sharing may be based on financial compensation necessary to balance the upstream investments of data holders. These situations would not accommodate the application of obligations imposing free transfers.

This sharing of data may also lead to subsequent exchanges of data with other public bodies or even third parties (Article 15 § 4 in particular). These exchanges can potentially go beyond the strict European framework and therefore undermine their competitiveness without conditions of reciprocity.

Many companies, active in public markets, also have public authorities as clients who may request access to data arising from an "exceptional need". It is proposed to better define the framework applying to these authorities (B2B or B2G).

The provision in the context of a "specific mission of public interest" (Article 15 - c) also seems disproportionate.

Finally, companies are surprised that the data holder is responsible for assessing the proportionality of the request for data from public bodies. This provision illustrates once again the ambiguity of this text which assimilates all types of data.

The scope of access to data by public authorities following "exceptional needs" should be clarified; sharing obligations towards public sector bodies (B2G) should be duly justified (no intervention when the current situation is satisfactory) in order to avoid extensive national interpretations that risk weakening companies. Similarly, it is proposed to better define the framework applying to public authorities in relation to private entities (B2B or B2G). Finally, the obligation of free transfers is likely to unduly destabilize the existing investment and commercial balances, to the detriment of the preservation of incentives to invest.

This framework must prevent any potential violation of data and intellectual property rights and ensure against cybersecurity risks and breaches of confidentiality. Data shared in this way must not become public. In general, the data holder should be able to refuse this sharing, when these guarantees are not ensured or respected.

Clarifications to be made on changes to data processing services (Chapter VI)

Chapter VI deals with the change in data processing services, supported by AFEP companies.

Facilitating the change of subcontractors through better data portability and increased interoperability in services will help **support innovation and competition** between economic players.

The **technical feasibility of such projects** must nevertheless be integrated into these provisions by specifying the responsibilities of the service providers among themselves (incoming and outgoing), the responsibilities of the customers and of these same suppliers or by affirming the contractual freedom of these actors in the concrete organization of these service changes (calendar, for example). The migration of large volumes of data hosted on multiple servers can indeed induce more or less long delays.

Others: safeguards in an international context and implementation and enforcement (Chapters VII and IX)

Chapter VII deals with non-personal data safeguards in an international context. Chapter IX discusses the implementation and execution of Data Act.

Chapter VII intends to enshrine the principle of European sovereignty in matters of non-personal data.

- The **proliferation of data processed** implies increased responsibility for data controllers and the risk of conflicts concerning the management of personal data.

- In this context, a **clarification of the role that should be incumbent on the public authorities** is necessary. As such, the task of studying the legal systems of third countries should fall to the public authorities.

- AFEP also recalls **the importance of data flows** from and to the EU for European companies and calls for avoiding new barriers and uncertainties in the market. As such, the burden on the data processing service provider to prevent international transfers (Article 27) appears disproportionate in view of the reality of these flows.

Finally, while Chapter IX aims to regulate the powers of the authorities responsible for applying and executing this regulation, companies emphasize their desire for **administrative simplification and consistency**.

Companies are particularly surprised by the **retroactive effect** of possible penalties or sanctions by these competent authorities (Article 31-3-d). The implementation of the Data Act will necessarily take a long time within companies (heaviness of data flows) - especially in large structures. Companies cannot be penalized for their efforts when this retroactivity is unframed and unspecified (regarding the period or the type of act concerned).

About AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority.

AFEP has 114 members. More than 8 million people are employed by AFEP companies and their annual combined turnover amounts to €2,600 billion.

AFEP is involved in drafting cross-sectoral legislation, at French and European level, in the following areas: economy, taxation, company law and corporate governance, corporate finance and financial markets, competition, intellectual property, digital, labour law and social protection, environment and energy, corporate social responsibility and trade.

Contact:
Emmanuelle Flament-Mascaret, Director for Economic Law / concurrence@afep.com
Alix Fontaine, European Affairs Advisor / a.fontaine@afep.com