23 May 2022

EBF_045685

EBF position on the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)

Key messages:

- The EBF welcomes the opportunity to comment on the Commission's proposal for a Data Act.
- While welcome, **the scope for new obligations** for data access from connected products and related services **needs to be clearly defined** to provide legal certainty for firms and effective enforcement of the Regulation. Provisions on aspects such as **data sharing modalities** are also needed to enable firms to leverage the new data access opportunities offered under the Act.
- The **compensation principle** under Chapter III is an important and needed step forward, recognizing the **investment by data holders**. Yet the possibility to limit or remove it must be done only in exceptional circumstances in order **to avoid asymmetries** between different data sharing frameworks, thereby nullifying their horizontal nature.
- For B2G data sharing, the **scope for the data access for exceptional need must be clearly defined**; the Act cannot become a fallback for public bodies to request data when there are existing supervisory and reporting frameworks that provide for it or an excessive use of data from companies without a control mechanism.
- Provisions under Chapter IV should take a proportionate approach, factoring in the different size of companies (and bargaining powers) and provide more details on how the unfairness test is to work in practice so as so avoid uncertainty in contractual negotiations.
- The EBF welcomes the European Commission's intention to address the challenge of lock-in effects for business customers of data processing providers. The endeavour to provide regulatory requirements to foster switching between cloud service providers needs to balance practical technological aspects with strategic considerations for cloud availability. Chapter VI, as well as corresponding definitions, would benefit from a number of clarifications and additions.

I. Introduction

The European Banking Federation (EBF) welcomes the opportunity to comment on the European Commission's proposal for a Data Act, and its overall objectives to increase opportunities for access and re-use of data. A **European data economy** which unlocks **new opportunities for customers** – individuals and firms – through increased access to and sharing of data is a priority that the European banking sector welcomes in **the process of its own continuing digital transformation**. It is the **combination of data from**

different sectors which holds the greatest potential for delivering new services and experiences for customers[1].

Therefore, while we support the new obligations on data access from connected products and related services (with a clearly defined scope), **the ineffectiveness of the existing right to portability is a problem for all data currently subject to this right, not only for machine-generated data –** which can **prevent the development of cross-sectoral data access use cases** (see use cases under footnote 1). The Act should be **more ambitious** on the sectors it opens up data access to; currently it falls short of introducing a real horizontal framework by stopping at access to connected product and related services data. Taking a sectoral approach risks generating fragmentation between the data access regimes to the detriment of the EU single market and to sectors which already have data sharing obligation (such as the banking sector).

As a pragmatic first step, the Act could include enhanced portability for data from telcos, utilities, and e-commerce, which would facilitate greater reuse of data across sectors and would open up further opportunities of new and improved products and services. The Data Act itself already provides for a possible extension of the scope in the assessment that will be carried out two years after its application.

The proposal also falls short when it comes to the **operationalisation** of the opportunities of data access and sharing **from IoT products and related services**. More details are needed on the **modalities for data sharing,** notably **secure access and transfer mechanisms, data formats, and secure communication**. In other words, while technical barriers are identified as one of the main obstacles to data sharing, the Act does not take the steps to remove them. This creates a risk of fragmentation among data sharing frameworks and actors, such as authorised third parties, **who are then unable or discouraged from developing new innovative services with this data**.

The Act's introduction of horizontal principles which not only apply to the current Regulation but to future initiatives is very welcome, particularly the **principle on compensation.** However, the ability of other legislation to limit or remove this possibility must only be undertaken **in exceptional circumstances**. If some sectoral frameworks allow compensation whereas others do not, **this could create asymmetries.** The situation under the revised Payment Services Directive (PSD2) is an example of this.

Regarding other chapters of the proposal, for Business to Government (B2G) data sharing the **scope for sharing data for "exceptional need in case of fulfilling a specific task in the public interest" is too broad** and needs to be further specified and the notion of "exceptional need" defined. It is also important to clarify the type of data to be shared by companies. Meanwhile, the chapter on unfair contract terms should consider a different approach for medium sized companies on one hand and small companies and microenterprises on the other since they share distinctive characteristics, such as differences in bargaining power. The scope of the data concerned by these terms should also be limited.

The EBF welcomes the European Commission's intention to address the challenge of lock-in effects for business customers of data processing providers. Safeguarding choices to change providers is important to allow businesses' proper access to innovation and to enable their execution of business strategies. In the financial sector, properly empowered financial institutions can provide cutting edge services to their customers and advance in the application of digital transformation tools. Adoption of cloud computing is a prominent example where a lock-in effect needs to be discussed.

---

[1] In the banking sector (which is already making core client data available under PSD2), for example:

- Data from e-commerce can enable banks to do more accurate and faster credit risk assessments for SMEs and expand access to finance for underserved segments.
- Data from transport-related purchases (e.g., vehicles, fuel, public transport tickets) could allow for recommendations on money-saving or greener options or help anticipate maintenance needs.
- Data from households on their energy use and property could facilitate the provision of advice on greener energy choices or green financing for renewable energy installation.

At the same time, cloud computing solutions are technologically complex. The endeavour to provide regulatory requirements to foster switching between cloud service providers needs to balance practical technological aspects with strategic considerations for cloud availability. For example, service designs for innovation uptake can be vendor specific. In turn, access to cloud innovation can be considerably impacted by the designed legal framework for cloud switching.

European banks consider both strategic dimension and practical perspective on cloud switching. We are looking forward to participating in the European discussion of regulatory requirements under Chapter VI of the Data Act. The implementation of these requirements needs to be carefully considered and we look forward to engaging with policy makers on the basis of our evolving understanding of regulatory intentions and impact on service implementation.

Today, European banks face a strict and comprehensive framework of banking regulation. They are dedicated to compliance with these rules, and in turn have to ensure their translation into contractual arrangements with CSPs. This can create **significant frictions** in contractual negotiations. Voluntary standard contractual clauses (SCCs) are another opportunity for the European Commission to address the friction. In expectance of respective work being conducted after finalization of the legislative negotiations of the Digital Operational Resilience Act (DORA), the EBF calls to the Commission to ensure alignment between requirements under the Data Act the final requirements for contractual elements under Art. 27 DORA and future SCCs. Consistency across these legislative and non-legislative tools is key for cloud users to secure compliance and avoid disproportionate burden by conflicting rules.

Finally, both the Data Act and Data Governance Act include provisions on developing interoperability – the interaction between them when it comes to interoperability and more generally, needs to be specified in the text to provide certainty to all actors.

II. Chapter II: B2B and B2C data sharing

a. Scope and definitions

The scope and definitions must be **as clear** and as **specific** as possible in order to avoid misunderstandings and to ensure effective enforcement of the Regulation.

While the text includes the definition of a "product", **a definition of a "connected product" is missing**. Since the field of connected objects is vast, particularly if we consider that all traditional, non-technological objects that are augmented by at least one sensor, chip or QR code, a clear definition of a "connected product" is important to provide legal certainty for companies.

This is also essential to enable the Regulation **to focus on the relevant connected products** for the data access obligations. For instance, **Point of Sale (PoS) systems, Automated Teller Machines (ATM), and bank cards should not fall under the scope of the product definition**. It would be important to clarify the exceptions as well (e.g., smartphones when used or repurposed to function as PoS systems). Their main purpose (primary function) **is not to generate or collect data concerning its use or environment, or to store and process data**; the Regulation should not apply to products that generate data as a result of intentional human input to display, record, or transmit content (Recital 15).

Services related to such devices should **not fall under the scope either**. Overall, it is important to **clearly lay out the notion of related services**, including the specific link to the product. For example, it is important to specify that data related to payments performed through wearables, for example, do not fall under the scope of related services as there is an existing regulatory framework for access to payment account data (PSD2). Banking apps should also fall out of scope. Notably, **the Commission clearly sets out in its current consultation on an Open Finance Framework that "*the recent Data***

Act proposal does not introduce any new data access rights in the financial sector[2].”

Virtual assistants are only in scope insofar as they are used to access or control a connected device, rather than being scoped in intrinsically. Thus, **since virtual assistants from the banking and financial services industry are not tied to a specific device**, they should be **out of the scope**.

Regarding the exclusion of SMEs and microenterprises from the scope of obligations, while we understand the reasons of administrative burden, it is important to consider that an SME can also be a large player in the data economy. Employee size is not a good measure in this regard. **The notion of the size of a company is not relevant for the respect of the level of play field.** More proportionality in the application could be achieved by limiting this exemption to microenterprises.

Clarify the definition of “providers of data processing services” under Art. 2(12): While Art. 2(12) defines “data processing service”, the Art. 23 and following refer to *providers* of such broadly defined services in particular. Art. 2 should incorporate a respective definition of who these providers are in the context of Chapter VI, introducing an explicit reference to cloud and edge service providers as covered entities. Today, data processing is – to a varying degree – a part of many business operations by different entities, and not necessarily restricted to cloud and edge service providers only. Where Chapter VI seeks to facilitate switching between mainly cloud and edge services (see Recital 69), clarity is required in the legal definitions.

Where private cloud services are offered by an entity for its inhouse use only, this entity should be explicitly excluded from the definition, since this constellation does not provide the same challenges for lock-in and market choice.

Missing definition of “metadata” in Art. 2: In Art. 24 and 29, the draft proposal refers to metadata. The obligations to include metadata in the exhaustive specification under the contract requires a legally certain understanding of its definition. The same is true for addressing application metadata portability. Hence, Art. 2 should include a respective definition of the term “metadata”.

Missing definition of “operator of a data space” in Art. 2: Art. 28 (1) introduces the terminology “operator of data spaces”. In the interest of legal clarity and security, this terminology should be defined under Art. 2, targeting the compliance with essential requirements under Art. 28(1) more clearly.

b. Type of data

Recital 14 of the proposal clearly states that “*…the data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information **derived or inferred from this data**, where lawfully held, **should not** be considered within this scope of this Regulation.”* We **support the distinction** made between **observed and provided** on the one hand and **inferred and derived** on the other as well as **the exclusion of the latter from the Regulation**. This exclusion ensures that users have control over their provided and observed data, while **protecting the value creation carried out by the data holder,** which may have inferred or derived further insights or information that they should not be obliged to share. Inferred / derived data must therefore remain in the sole availability of the data holder in order to safeguard intellectual property. We therefore recommend to **include this exclusion in the Articles themselves** and not only in the recitals.

In addition, we would recommend a clarification from the Commission on what type of data falls within observed data under the Regulation, particularly with regards to non-

[2] European Commission, Targeted Consultation on Open Finance Framework and Data Sharing in the Financial Sector, 2022, p.3

personal data.

c. Specifying modalities for data sharing

We support that under the Act, **users are both legal and natural persons** as both stand to benefit from data sharing opportunities and the new services that could come from them. The ability for users to share data with third parties is also very welcome. By enabling this, the Act recognizes the value added that different actors can bring to customers, as well as **the value of combining data from different sectors** since, with the exception of companies designated as gatekeepers under the Digital Markets Act, there is no closed list of eligible third parties.

Regarding the **modalities of data sharing**, the proposal says that the data holder shall *make available to the user the data generated by its use of a product or related service without undue delay, free of charge, and where applicable, continuously and in real time*. This should be done on the basis of a simple request through electronic means where technically feasible. In our view, the **operationalization of the data access possibilities needs to be further specified,** as the proposal **lacks detailed provisions on the need to develop secure access and transfer mechanisms, secure communication channels and management of consent.**

Without further specification, **we see three big risks emerging:**

1. Market actors' inability to leverage the opportunities offered by the Act to deliver new services to customers.
2. A threat of fragmentation and maintenance of data silos between industries.
3. The lack of operationalisation could result in high costs especially for SMEs.

In terms of **secure data sharing mechanisms, APIs** are a potential tool to consider, as they help guarantee maximum interaction, remove entrance barriers and enable secure and real time direct data access and exchange between the data controller and the receiving company/user as a pre-requisite for offering integrated services to customer which provide real benefits. However, the Act should **allow for the development of other mechanisms** that enable real time, secure data exchange, as requested by customers in **accordance with the evolution of technology.** It should also take into account work already done in different sectors, such as the development of APIs by banks under PSD2.

The proposal puts forward **smart contracts** as a potential tool for data sharing, without mentioning others. Singling this tool out without considering existing mechanisms (or requirements for specific sectors, such as the banking sector after PSD2) could, as mentioned above, prevent the efficient development of the data sharing ecosystem.

In addition, the definition of smart contracts offered in the Act is too broad. **Smart contracts need to be clearly defined** in terms of:

- Who gets to issue them;
- Who identifies and is liable for transacting parties' responsibilities;
- Where and by whom the "smart contract" is executed.

Ultimately these are computer processes that automate an outcome based on predefined conditions between two or more parties. It makes all the difference who oversees that the process is executed as defined, triggering the question of liability.

Standardization also remains absent from the chapter. Multiple standards on data formats, exchange protocols, security (authentication requirements and secure communication) for different products will **result in complexities**. It could also lead to **additional costs and uncertainty** on the side of the data holders, whilst also preventing data sharing and interoperability on a larger scale, which is key in terms of building the

EU Single Market for Data.

Finally, under Art.4 and Art. 6, it is noted that *trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets and to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party, respectively*. However, in certain situations this may not be possible.

Competitively sensitive data may be the subject of the right for data access and sharing. **Sharing of data that allows conclusions to be drawn about specific competitive behaviour** (e.g. price information, customer-specific information, sales figures, capacities, developments, strategic planning) is **prohibited due to Art. 101 TFEU**. As a consequence, a data holder may have to deny access to certain data due to Art. 101 TFEU and, vice versa, data recipients may have to refuse acceptance or take internal measures (e.g. complete separation from business operations). In practice, there may be considerable difficulties in determining, which data can be legally shared without violating competition law.

d. Interplay with the GDPR

The proposal should elaborate on the interplay between the Data Act and the GDPR. For example, the provisions on information obligations toward the data subject, the information obligation to ensure transparency, etc – how do these interact with the provisions under the GDPR? Duplication must be avoided. In this regard, definitions used under both Regulations should be aligned.

We would also welcome a clarification on the applicable legal basis under the GDPR for end users to share data with third parties. This is an areas where guidelines could also be useful. If these are produced, coordination between the different relevant authorities, notably the European Data Protection Board (EDPB) is essential, to avoid confusion later on. In the financial sector, the experience with the EDPB's Guidelines on the interplay between the GDPR and revised Payment Services Directive (PSD2) and the lack of alignment between different authorities continues to raise concerns. This should be avoided with the Data Act.

III. Chapter III: Obligations for data holders legally obliged to make data available

a. Maintaining a strong compensation principle

We support that there is, at least, a **general horizontal approach (although very basic) to data sharing obligations,** also for those established in **future legislation.** Particularly, we support the provision under **Art.9** that establishes **the possibility of receiving reasonable compensation** for making the data available. A fair **distribution of value** is key in terms of **providing incentives for data holders** to invest in data and this principle should apply to future sectoral initiatives such as Open Finance. However, the fact that Art. 9(3) allows that other Union law or national legislation implementing Union law could exclude compensation or provide for lower compensation for making data available **may lead to market asymmetries and incoherence** between sectoral frameworks.

The current regime under PSD2 where access by some market participants to data held by other market participants takes place free of charge, creating a situation where there is no fair distribution of value, is an example of the risk of asymmetry.

The possibility to exclude compensation for making data available or to provide it for lower compensation **should therefore only be allowed in exceptional circumstances and should be duly justified.** For example, the Digital Markets Act does not include compensation under the obligations touching on data access (Art. 6(1)(h) and 6(1)(i))

however it is within a specific context and meets the objectives of this Regulation (the DMA).

b. Additional comments

In Art. 8(1), the Act states that "*where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and* ***non-discriminatory terms*** *and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV."* Different data recipients could have their own interpretations of what qualifies as "non-discriminatory" terms. If the principles under this chapter are to be horizontal, the Data Act should indicate what is meant by the term with regards to data sharing to provide certainty for data holders and data recipients across all sectors.

Art. 8 (3) of the proposal states that the data holder "*shall not discriminate between comparable categories of data recipients*." What is understood by **"comparable categories of data recipients"** needs to be clarified further.

We would also recommend a clarification on the interaction between Art. 8 and Art. 40 of the proposal. Art. 8 does not limit the scope of the Article, but Art. 40 notes that "*The specific obligations for the making available of data between businesses, between businesses and consumers, and on exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before [xx XXX xxx], and delegated or implementing acts based thereupon, shall remain unaffected."* It should be clear that there is no retroactive effect.

IV. Chapter IV: Unfair terms related to data access and use between enterprises

We have some concerns in relation to **Art. 13**, which establishes that a contractual term unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise shall not be binding on the latter enterprise if it is unfair. Specifically:

- In relation to the subjective scope of this chapter, we believe that micro and small companies have **different characteristics** (and a different level of bargaining power) **from medium-sized companies**, for which the **approach should be different** in the application of the requirements. The principle of **proportionality** should be applied.
- Regarding the objective scope, we consider that **data necessary for the performance of a contract** to which the **data subject is a party** should be **out of the scope** of this chapter.
- As per Art. 13(4), we believe that the **conditions** presuming that the contractual term is unfair are **vague and subject to different interpretations**, which creates uncertainty for contract negotiations. Also, who would the parties turn to in case of a disagreement? This question points to the fact that it is very unclear how the unfairness test introduced under the Article is intended to work in practice as the whole concept of "fairness" of contractual terms is subject to contracting parties' individual interpretations.
- The Art. 13(5) provision which outlines that the contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed is challenging, as some of the negotiations may be verbal and this would represent an additional administrative burden to those a company already has and could result in conflicting interpretations.

We would like to underline that **freedom of contract is the clear underlying principle of contract law in most European jurisdictions in B2B relations.** Any exceptions to its scope of application and the conditions for the unfairness test must **therefore be clearly defined.** Contracting parties need more certainty and clear guidance what terms

could be regarded as "excessive and abusive" and therefore invalid, and who has the power to take a decision on their "unfairness" as the last resort.

Finally, it is important to note that the situations described in the chapter are also encountered by companies of all sizes (e.g. when negotiations with large technology providers). The provisions of the Digital Markets Act capture some of these practices when it comes to undertakings designated as gatekeepers and it is important to acknowledge this in the Data Act proposal.

V. Chapter V: Making data available to public sector bodies and union institutions, agencies or bodies on exceptional need

As a general comment, the public sector already has broad powers to request data or information from the private sector. Often these powers are subject to checks and balances. Introducing additional powers must be carefully examined to prevent unintended consequences and duplication.

a. Clarify scope of "exceptional need" where the lack of available data prevents the public sector body from fulfilling a specific task in the public interest

The obligation to make data available when the ***exceptional need*** *is the lack of available data preventing the public sector body from fulfilling a specific task in the public interest* **could be problematic, as the scope of this circumstance is too wide, and open to interpretation**. It is important to define the notion of "exceptional need" and it is paramount that the situations remain – as in the title – "exceptional." Also, **proportionality** and **a clear legal basis** should be the principle that inspires any obligation to oblige data holders to provide data to the public sector.

There are several fields where public authorities already have comprehensive rights to be granted access to various data in order to fulfil their assigned responsibilities. This applies especially to supervisory authorities in the financial sector for the purpose of safeguarding financial stability. It should be clarified that in these cases, **where legal bases already exist, the provisions of this regulation should not apply.** Reporting provisions in the financial sector are some of the highest; the Data Act should not become a tool that public authorities resort to if they are not able to get data under established frameworks and structures, even though the latter provide for it.

In addition, current reporting requirements are based on clear mandates. The existing obligations **could potentially create a very open-ended basis** for additional supervisory requirements outside of the current supervisory mandate.

Regarding data provision **in case of public emergencies**, it is important to clarify **how existing cybersecurity incident reporting obligations** such as those under the Digital Operational Resilience Act (DORA) and Revised Network and Information Security Directive (NIS2) **would interact with responding to major cybersecurity incidents**, which are included in the list of human induced disasters (Recital 57).

Art. 21(1) states that a public sector body shall be entitled to share data received with individuals or organizations 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. **In the case of personal data, this provision may contradict the GDPR,** which has strict provisions on data processing for another purpose different for which the personal data are initially collected. In this case the controller must consider several factors before sharing those data with individuals or organizations.

Finally, we see it as problematic that there is no need **for a neutral and legitimised body** to decide on the proportionality of data access, such as the legislator or the courts. If the decision lies with the public body that has an interest in collecting the data, **this**

can lead to excessive use of the data from companies without a control mechanism. There is also an increased risk of misuse or breach of sensitive data. Moreover, it is unclear what criteria are used to select companies to provide the data.

b. Specify what type of data is to be shared

Article 17 sets out what a public sector body or a Union institution/agency/ or body needs to include in a data request. Still, there is no indication of **what type of data could be part of the request.** For example, is it raw data or derived data as well? For example, when it comes to cybersecurity, there is a distinction between the raw data and interpretation and estimation. What is the consequence if the data shared is not accurate (due to the stage of analysis it is at)?

We also query how this complies with bank's professional secrecy obligations. This must be specified in the text. More generally, the GDPR may restrict types of data to be shared; a legal basis needs to be introduced to allow the sharing of any type of data in scope of the Art. 17 obligation. As a minimum, **EU regulators should make it clear which type of data is subject to the obligation in Art 17.** However, on a practical note, any grouping must be practical for controllers. There are already practical challenges for banks when ensuring data linage based on GDPR data categories.

c. Workable deadlines

The current deadlines under Art. 18 to make the data available will be very difficult to implement in practice if the scope of the data to be provided is not clearly specified. First banks will need to identify it in their respective systems (data linage), then they will need to technically convert it into a format which is readable to the authorities, and then banks need to have a secure channel by which to can send it to the authorities. This also brings up the question of a secure line of communication with the authorities to share the data.

d. Compensation

While data holders may request compensation when providing data under the exceptional need case, **it should be possible to request compensation for all cases under this Chapter, including for public emergencies**. The investment and effort to provide the data does not change whether it is for a public emergency or for the exceptional need case.

V. Chapter VI: Switching between data processing services

a. Art. 24: Mandatory transition periods of maximum 30 calendar days

The mandatory transition periods defined in paragraph 1(a) and (c) are too specific and require an option for cloud users to flexibly agree on possible extensions. In a complex setup of a cloud environment, switching needs to consider not only the actions required by the provider, but also the planning, coordination, and operation by the cloud user. The timeframe required to migrate to another provider or back to internal premises will vary depending on the complexity of the service.

The time required to exit a service is directly related to the complexity of the service. While for IaaS or CaaS services a maximum period of 6 months might appear reasonable, more time would be required for complex SaaS services. The time for transition will depend not only on the service provider but also on the capabilities of the customer. Under the Data Act Chapter VI, contracts should be able to include the **right of the cloud user to request or agree to a longer transition period** if needed (e.g. due to a service's

complexity) and the **possibility to request or agree to extensions** if necessary, during which the provider obligations set out in Art. 24(1)(a) shall apply.

If not, there is a risk that EU users of cloud services, including banks, could be forced to simplify their cloud deployments, thereby limiting the value of using cloud. This would put them at a disadvantage to users in other jurisdictions and obstruct the way to EU leadership in digital service.

b. Art. 24(1)(b): Minimum data for export

European banks welcome the flexibility to apply Art. 24(1)(b) according to relevant cloud scenario and service usage. Where data and applicable application categories are exhaustively specified, such analysis gives room for consideration of the individual case of cloud use in question.

Catering to the need for flexible application of the requirement, the interactions of end users with the service should be included among the minimum metadata that should be exported under Art. 24(1)(b). In the case of SaaS, this information is especially relevant, because it allows, for example, to identify which services are the most used, the least used, how many times they interact and what usage patterns exist.

Art. 24(1)(b) introduces two cumulative criteria for relevant metadata specification: created by the customer and by the use of the service during the period the service was provided. Since metadata – missing a definition under the Data Act – may be hard to trace to the customer as originating source, the paragraph should be amended:

"[...] metadata created by the customer **or** by the use of the service [...]".

However, it will be difficult to specify all metadata to be ported in the contract itself as such data will be continuously created through the use of the service. The term "exhaustive specification" therefore may not allow users the necessary flexibility to negotiate their contracts in a way that fits the service being provided.

c. Art. 24(1): right for data deletion

Providers of cloud and edge services should be required to permanently delete user data, following a successful switch to another provider or back on-premises by the user. The provider should propose a concept for data deletion – covering both logical and physical aspects – for inclusion in the contract. Users require a right to amend this concept as part of the contractual negotiations, reflecting on their specific requirements and needs.

This right for deletion is particularly important, since Art. 24 addresses all data, including backup sets, off-site backups, historical data kept for required data retention and encryption keys (current and past).

d. Art. 26(4): Additional tools required from providers

European banks welcome that the proposal refers not only to the data but also to the relevant data formats and data structures. Cloud users usually do not know how the data is organized, particularly in SaaS services. It would therefore be necessary that the data processing service also provides technical tools that enable cloud users to exploit and migrate this information to an alternative service provider.

VI. Chapter VII: International contexts non-personal data safeguards

European banks support that providers of data processing services take all reasonable technical, legal, and organizational measures to ensure the security, confidentiality and

protection of data, including non-personal data. It is important to preserve a company's trade secrets and intellectual property.

It will be key that the European Data Innovation Board coordinates with data protection authorities that extensively regulate international data transfers when they involve personal data. Any guidance for non-personal data should be consistent with the GDPR.

European banks appreciate a chance to continue exchanges on details of procedural questions under Art. 27.

VII. Chapter VIII: Interoperability

For individuals and businesses, improving interoperability is important. For example, it reduces the dependency on a provider and makes it easier to switch to another provider or execute an exit scenario. Interoperability requires obligations on all service providers, the incumbent service provider as well as potential successor service providers, to ensure services can be easily moved around without impact on functionality, integrity and availability.

Although the interoperability chapter already includes essential requirements regarding interoperability of Data Spaces, European banks consider additional guidance by the Commission helpful to provide specifications to the requirements and place them in the legislative landscape addressing data. In particular, we would recommend **a clarification on the interaction between the provisions on interoperability under the Data Governance Act and the Data Act.** In the former, under Art. 27(d) the European Data Innovation Board (EDIB) would assist the Commission in tackling fragmentation by addressing cross-border and cross-sectoral interoperability of data, and, under Art. 27(da)(ii) proposing guidelines for common European data spaces on, among other points, requirements for ensuring interoperability.

At the same time, under Art. 28 of the Data Act sets out essential requirements regarding interoperability for operators of data spaces. **How will the essential requirements fit in with the future guidelines the EDIB will produce?** The same applies for any future sectoral initiatives which will include provisions on interoperability.

Finally, Art. 28(1) mentions **"operators of data spaces"** , but it is not clear what the concept of data spaces entails also due to a missing definition and who the operators are as the common European data spaces would probably be designed differently with different actors coming together to share data.

VIII. Chapter IX: Implementation and Enforcement

In Chapter IX, member states have been given the possibility to introduce a new competent authority. This might lead to the situation that even more guidelines, Q&A's and other forms of soft law are introduced. It could therefore be useful to include a provision that competent authorities should coordinate any Guidelines under the Act.

IX. Chapter X: Sui Generis Right under Directive 1996/9/EC

There should be a reflection to find a more balanced dividing line between what is proposed in the Data Act and the sui generis right under Directive 1996/9/EC. The current right is a powerful complement to Intellectual Property rights. As a result, we are worried that Article 35 de facto challenges the existence of such right in any database where only one data point, for example, is "obtained from or generated by the use of a product or a related service". At best, such a provision is bound to hinder the evolution of databases and prevent developments including such data, which is not the aim of the text.

X. Conclusion

The Data Act does take an important step forward in terms of increasing access to and sharing of data across the EU. However, the proposal also contains shortcomings which must be addressed if this goal is to be achieved. These include expanding on the modalities for data sharing when it comes to IoT product data and related services data; ensuring that the possibility to limit or exclude compensation for data holders under Chapter III is allowed only in duly justified, exceptional circumstances; defining and clarifying the scope of "exceptional need" under the B2G chapter; and ensuring that the chapter on unfair contractual terms is targeted. Leaving these points unaddressed risks depriving organisations of the opportunities offered by the Act and, on other points, creating legal uncertainty for all stakeholders in the data economy.

For more information:
Julian Schmücker
Senior Policy Adviser – Digital Innovation
j.schmucker@ebf.eu

Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu