

EBF_041452

31 May 2020

Annex to the EBF's consultation response on the European Commission Data Strategy

Considering the – often – complex discussion and necessary understanding of data related technological innovation, the character limits in the response template may not give sufficient opportunity to provide feedback within the proper context. To provide such essential context, ultimately allowing the reader a better overview and understanding of the issues in question, the EBF invites the Commission to consider the following Annex. It shall be read complementary and as expanding on, the answers provided in the survey.

Introduction

The European Banking Federation (EBF) supports the European Commission's ambition to create a single market for data in the EU. If effectively implemented, the Strategy is a first step to promote a European Data Economy that benefits both consumers and firms.

The greatest opportunities for data-driven innovation will come from reusing and combining data, particularly across sectors. This is being underscored by the current Covid-19 crisis (e.g. importance of telecoms or mobility data to address challenges in the health sector). As the Commission outlines in its Data Strategy, "*making more data available and improving the way in which data is used is essential for tackling societal, climate and environment -related challenges.*" In addition, the proposal for a Green Data Space shows the importance of creating an ecosystem of data that is not limited to sectoral boundaries.

Most importantly, **users should be at the centre of the data economy** and regulatory initiatives should directly help individuals *and* firms to take control over their data in the digital environment -- how it is used and how it is shared.

The EU has the opportunity to regain competitiveness with respect to other jurisdictions by, as viewed by most EBF members, enhancing the existing portability right for individuals under Article 20 GDPR and working towards a suitable data portability right for firms. This would stimulate innovation and competition for the benefit of both end-users and industry.

Comments on different initiatives and elements of the Data Strategy and consultation follow.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

1. EU Common Data Spaces

We understand that Data Spaces are a way of organising initiatives around key sectors and policy priorities and we support work to encourage data exchange and reuse. Yet, **we would like to underline that data is especially valuable across sectors, particularly to spur the innovation which the European Commission envisions in its Data, AI and overarching Digital Strategies.**

For example, data from a Green Deal Data Space could be used by financial institutions as they support their customers green transition, including to enhance climate change risk assessments or analyse green loans. The Strategy already notes that the potential cross-sector use of data between sectors needs to be taken into account. This should be expanded, **and the Data Spaces initiatives should start from the principle of making all data available on a cross-sectoral basis** (with necessary controls and licensing wherever appropriate).

In the strategy, the proposals are very high level. We agree with the Commission's approach to largely leave the work on the Financial Data Space to be driven by the Digital Finance work stream. However, as noted in our survey response, we recommend that cross-sectoral data-sharing and use-cases should be factored into all data space development.

We would also like to ask for clarity as to how the horizontal governance framework for common EU data spaces will look like and what it will aim to achieve and **recommend the Commission to take into account the following points in its elaboration:**

- Participation in Data Spaces on a voluntary basis can be a suitable way forward, providing initiatives on implementing effective portability for users on a cross-sector basis are also in place, as set out below.
- In its communication, the Commission states that these European data pools may be organised in a centralised or a distributed way. We are of the opinion that **centralised structures should not be the default option as it is important to make data accessible but without having to duplicate it.** Given their creation cost, it is not certain that potential common centralised infrastructures would bring real added value.
- **Security and data protection need to be key elements of the creation of data spaces,** to minimise the risks of cyber-attacks and data security breaches outside and create trust among those firms who wish to participate, in any of the sectoral data spaces.
- The horizontal framework **should consider how data spaces will interact together,** as availability of data between sectors is likely to be a key enabler of innovation.
- Given the complexities of establishing Common Data Spaces and its impact on other key initiatives of the EU's Digital Strategy (AI adoption, data access/re-usability, etc.), the relevant authorities should be empowered to ensure a coordinated implementation across the key sectors identified.

2. Data sharing for individuals and firms

As set out in the [EBF policy paper on Data Usage, Access and Sharing in the Digital Economy](#) in January 2020, the EU's ambition should be for a cross-sectoral regulatory framework to unlock the real benefits of data cross-fertilisation for the digital economy. The key to unlock this, as seen by most EBF members, is to make data portability fit for the 21st Century, so that it works for the European data economy. This would empower users - individuals and firms -, enhance competition and support data-driven innovation.

A number of initiatives proposed in the Digital and Data strategies offer a first, practical step towards achieving this.

a) Empowering individuals

To empower individuals, the European Commission should focus on enhancing the existing portability right for individuals under Article 20 of the GDPR through the Data Act, as outlined in the Strategy, so that it is actionable and practical.

Recognising the complexities of implementing enhanced portability for all firms and datasets in the short term, **the Data Act should focus on requiring enhanced personal data portability for a subset of organisations holding data of particular value to individuals.** This should include data from:

- Digital platform providers (e.g. e-commerce, social media, streaming, mobility service);
- Telecommunications providers;
- Utilities (e.g. gas, electric, water); and
- Public authorities (such as public registries, tax, and social contributions data).

All actors must ensure that privacy rules are abided at all times, also when considering any further use of such data.

b) Empowering firms

The Commission should also work towards a suitable data portability right for firms in a similar way to the inclusion of business accounts in PSD2 (ensuring this is designed to protect intellectual property and personal data rights). **There is an opportunity to start with business user's data held in significant digital platforms.** A first step towards this should be taken as part of the development of ex ante rules for markets with large digital platforms, planned for the Digital Services Act.

An increasing number of firms depend on and transact through digital platforms, making the data stored in these platforms critical to business users. Enabling users to transfer their data from the original service provider to another firm would increase competition and allow data to be reused across other sectors. To implement this, new ex ante rules should require large digital platforms to offer their business users portability tools that allow them to share and transfer their data, within the frame of firm data protection and other relevant legislation.

In parallel, the initiatives in the Data Act to clarify firms' rights over data (particularly where it is co-generated) can also help to provide firms with effective portability of their data. Both initiatives should ensure that users -whether individuals or firms - can **share the data they generate in a way that is easy, secure, in real time and on a repeated basis, through standardised interfaces such as APIs.**

c) Proposed actions

While partnerships are a valid way to gain access to some of the necessary data, all EBF members except one¹ do not think a voluntary approach to data portability will be sufficient to create a fair, open data economy. Misaligned incentives, coordination challenges, and imbalances in market power have meant that users have not been empowered in the past - whether in the financial, automotive or electricity sectors - until policy initiatives unlocked the opportunity for them.

To overcome these challenges and implement portability that is easy to use, secure and in real-time, **we recommend that initiatives mentioned in the Data Strategy - including enhancing the existing portability under Article 20 of the GDPR in the Data Act and ex-ante rules for digital platforms in the Digital Services Act - include the following:**

- **User at the centre:** users (consumers and businesses) should be empowered to decide which data to share and with whom within the frame of user and firm data protection laws (GDPR and other national data protection laws; competition laws, intellectual property, business secrecy, banking secrecy...). It is also important to help consumers to provide this access in a simple and non-binding way and to ensure that they are aware of and responsible for their choice.
- **Transfer mechanism:** standard dedicated interfaces (i.e. APIs) for key data sets, with real-time data transfer that can take place on a one-off or recurrent basis.
- **Security:** Authentication requirements (such as two factor authentication) and secure communication.
- **Standardisation:** Data formats, security, API models and user experience to be standardised, for example through industry standards validated by an appropriate governance structure, with input from EU and national authorities. Where appropriate, globally recognized standards should be encouraged. Constraints and requirements specific to the banking sector should be taken into consideration (e.g. EBA guidelines).

More broadly, we recognise the important role governments / the Commission can play in coordinating action by industry, for example to develop common standards that will facilitate innovation. **However, governments / the Commission should be careful not to try to micromanage this work or to define standards directly**

- **Licensing and liability/redress:** A full authorisation scheme similar to that in PSD2 could create unnecessary burdens if data is less sensitive. A proportional approach could require firms wishing to access data on behalf of users to register with authorities, use appropriate security certificates, and include a framework for resolving questions of liability and redress.
- **Cost recovery:** Firms should be able to recoup the cost of developing and maintaining portability APIs, providing this principle is applied equally and fairly across firms and sectors.

¹ Who support a voluntary approach based on partnerships through contractual arrangements.

It is important to note that firms also build value on top of raw or observed data, e.g. through analysis, data validation. Firms should be able to retain and build on this value. **As such, sharing of derived and inferred data should not in general be made mandatory or included in portability.** We caution against the risk that initiatives compelling the sharing of inferred or 'non-raw' data **could also inadvertently stifle innovation and competition.**

Inferred or derived data constitutes a crucial strategic and economic asset and is a strong element of competitiveness for companies. It therefore cannot be considered as freely and automatically accessible to third parties, as they need financial, technical, and human investments. Moreover, banks are often legally required to guarantee a higher quality of data (e.g. for Anti-Money Laundering, credit facilitation etc.). These processes create an additional layer of value on top of the raw data that should be recognized and valued.

Finally, we also recommend that all initiatives are accompanied by in-depth impact assessments to explore which additional organisations personal data portability should be required from in the future, in addition to the ones mentioned above, and reflect on how to ensure fair-cost sharing across sectors.

3. Re-use of Public Sector Data

The public sector in Europe has a central role to play in empowering users and facilitating the reuse of data.

First, it holds specific information on individuals and firms generated through their interactions with the state and public services. For example, tax and social security contributions, driving license information, and proof of residency. Individuals and firms should be able to share their data held in the public sector with the private sector, whether to ease administrative processes (such as sharing their tax data with their accountant), or to leverage it to receive innovative new services (such as investment recommendations based on their social security contributions).

One way to implement this is through enhancing existing individuals' personal data portability, under Article 20 GDPR, and through new initiatives to address the portability of firms' data. Governments should start with the data where portability is likely to render the most advantages to users, such as tax and social security contributions.

Second, the public sector holds huge amounts of data of wider economic, scientific, and social value. Some of this is already made available today: a selection of member states and institutions have created data sharing portals and started to increase the amount of data that is published. However, there is still much more that can be done.

The banking industry is a user of public data (e.g. meteorological data for its insurance business) and recognizes its potential for the development of data enabled financial service offerings. The EU has taken a step towards better availability of public data with the Open Data Directive. **We encourage the Commission to be ambitious as it defines relevant high-value data sets and recommend the use of APIs for data exchange with the public sector, to allow secure, real time data transfer across different firms².**

² On a practical level, the French "Etablab" experience can provide input to the Commission's ongoing work to make more public sector data available.

In this context we also encourage the Commission to follow the differentiation between raw data and elaborated/inferred data, so it does not disclose all the specific data that the financial sector shares with its relevant authorities in the supervisory context.

Data generated or held by individuals or firms may sometimes be able to contribute to the public good. As indicated in the data strategy, this could take place under different models, including data altruism (where individuals “donate” their data), and models of business-to-government data sharing. The review and potential implementation of recommendations of the High Level Expert Group on Business-to-Government (B2G) data sharing should be done in full consultation with industry, with particular care taken to ensure that any sharing does not impose unnecessary burdens on firms.

4. Cloud computing

The EBF welcomes the dedication of the European Commission to foster cloud adoption in Europe. The European Cloud Federation initiative and the cloud rulebook follow a commendable strive for European leadership in technology and respective infrastructure at the global level. However, the promotion of European cloud solutions should always consider fair competition and aim for increasing the range of cloud services available to European industries. Consequently, such strive should not impose restrictions or obstacles to the use of non-EU cloud service providers. Looking at the market reality, European industries require the option to utilize all competing service providers according to their own choice.

Legal clarity and certainty are of outmost importance for banks engaging in the process of cloud adoption. European banks are dedicated to their responsibilities created by a strict regulatory framework for the financial industry. The careful adoption of cloud technology by banks therefore can only move as fast as the necessary considerations of appropriate protection and security.

When the consultation’s Question 35 asks for a *feeling* of security and protection regarding sensitive data, one has to acknowledge European banks strategic approach to consideration of cloud use. It pays careful attention to regulatory compliance. However, the technological cloud reality introduces a shared controls landscape between CSPs and banks. Consequently, any perception of protection must acknowledge the necessary interaction between both sides when safeguarding data. In turn, perception can depend on the possibility for

- initial assessments by banks of the CSP,
- legal constitution of safeguards with effect throughout the cloud service (contractual setup) and
- auditing.

Before acquiring a cloud service, banks perform a security assessment of the cloud provider in question. Such assessment can utilize international standards and existing cross-industry guidance on security, e.g. cloud control matrixes.

Following a positive outcome, the continuing compliance and upheld security of the provider during a long-term service relationship is important. Key supervisory requirements of the EBA Guidelines on outsourcing must be reflected in the agreement of both parties. Therefore, it is important to have a fair contractual negotiation between CSPs

and banks seeking their cloud services. The EBF observes that the legal and regulatory constraints and the higher compliance risk derived from the use, management and storage of customer information constrain the adoption of cloud service models by a strictly (and comprehensively) regulated banking industry.

These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks as cloud service customers and CSPs. Standardization by way of model contractual clauses for cloud use are an appropriate tool to safeguard the proportionate implementation of requirements under the EBA Guidelines on outsourcing regarding cloud. Concrete problems experienced by banks can be found in the EBF recommendation paper on model contractual clauses (uploaded together with this Annex). The EBF believes in the value of incentivising the use of standard contractual clauses for cloud, welcoming the European Commission's dedication under the 2018 FinTech Action Plan. Looking forward to proportionate standard clauses in 2020 – with anticipated positive impact on contractual negotiations thereafter – future European cloud initiatives, such as a cloud marketplace, could take further account of this tool of contractual standardization.

Auditing rights, as required by the EBA GL, provide for an essential tool for banks to safeguard compliance in the cloud services facilitated by the CSPs. Consequently, European banks recommend dedicated model contractual clauses to ensure appropriate audit and access rights. For details please consider the EBF recommendation paper on model contractual clauses (uploaded).

Looking at sensitive data, knowledge of potential data access at the cloud service providers (e.g. by public authorities, see example of US Cloud Act) is important for cloud service customers' feeling of protection. European banks are dedicated to the existing responsibilities under GDPR. In turn, contractual arrangements with CSPs must reflect the data protection requirements that European banks comply with, giving sufficient basis to enforce potentially shortfalls.

Financial institution's considerations of regulatory compliance require a strategic approach to cloud usage, carefully securing banks' existing responsibilities for customers and financial stability. Such strategic and policy considerations – conducted before the adoption of the cloud service – later on also affect the work and selection of different providers. Sufficient time is needed by banks in case of service termination and transition to a new service provider (or inhouse solution) without negatively impacting service level and business. The limited standardisation and complexity of data migration to other providers further contribute to the need for time and assistants from the providers' side (business continuity, exit support).

Time is of the essence in establishing a globally competitive EU data ecosystem that is aligned with European values. Therefore, from the very start of the initiative it is crucial that European authorities have a clear mandate to implement a holistic and interoperable approach to standardize data and enabling technology infrastructures across sectors and borders.

To prevent regulatory fragmentation, the EBF encourages regulatory authorities to promote an EU-wide harmonized approach to supervisory requirements on cloud adoption, reducing fragmentation in supervisory practices in implementation of the 2019 EBA Guidelines on outsourcing. The EBF Cloud Banking Forum stands ready to assist and to offer technical guidance to foster the exchange between regulators, banks, and cloud providers (e.g. by technical papers on key issues for harmonization).

ENDS