EBF key messages to the European Commission's consultation on building the European data economy

26 April 2017

EBF_026840

EUROPEAN BANKING FEDERATION'S KEY MESSAGES ON BUILDING THE EUROPEAN DATA ECONOMY'S CONSULTATION

Data is growing exponentially, in terms of use, variety, volume and velocity. Data is at the centre of the digital revolution and consequently data analytics is increasingly creating new opportunities both for consumers, who can benefit from more innovative and tailored products and services adapted to their needs, and for companies able to develop new innovative businesses.

A number of challenges though, remain, arising from the misuse of data, information asymmetries and data security. Such concerns are taken seriously by the banking industry, as trust and integrity are its biggest assets. Confidence in banks as trusted parties is essential for their reputation and business model, a fact which adds to the effort and investments put into maintaining and improving setups, guaranteeing the safety of customer data.

The benefits of digitalisation can only be reaped if each and every stakeholder follows the same rules, and if the financial services' industry can apply data-based innovation in a clear regulatory environment that is the same for all players.

The importance of having an appropriate competitive environment with a level playing field for all the different players should be the main reason for ensuring that not only banks have to comply with high standards in order to use personal data.

This level playing field needs to be achieved both:

- within the EU between different types of firms, e.g. banks and non-banks; and
- between EU and non-EU firms.

Stricter European rules should not inhibit EU firms' ability to innovate, to operate dynamically, to use innovative data services and to direct services to targeted market segments if their competitors from outside the EU can serve European customers without similar restrictions.

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

www.ebf.eu

If we agree that data is the most valuable asset in the digital world, helping European players to deploy the highest capabilities in data is essential in order to guarantee their competitiveness. The success of the Digital Single Market inevitably depends on it. As a result, any regulatory development in the field of data should guarantee that players be allowed to extract value from the work they perform with data, while preserving data protection and the privacy rights for consumers.

Further consideration should also be given to enhancing the cooperation between the competent authorities regarding cybersecurity, data sharing, or to ensuring further legal certainty in the interpretation of the General Data Protection Regulation (GDPR).

It is our understanding that only non-personal data is considered in the current European Commission's consultation on "building a European data economy". In our view the issue of data should be considered as a whole (personal and non-personal) by the European Commission in the Digital Single Market Strategy (without challenging the fact that non-personal data is outside of the scope of the GDPR).

1. LOCALISATION OF DATA FOR STORAGE AND/OR PROCESSING PURPOSES

Data flows are an integral part of companies' daily trade and operations. Their ability to transfer data throughout the world is vital including for banks, no matter their size or the geographic area in which they operate.

We observe that one of the hindrances to a consistent European Union (EU) and Global regulatory framework for Cloud Computing in Financial Services is related to regulation and domestic laws which establish barriers to the geographic location of the physical Cloud Computing infrastructure. Frictions to leveraging the benefits of Cloud Computing in Financial Services arise when data regimes restrict cross-border data flows, both within the EU and globally.

Data stored in a Cloud Computing environment can be fragmented geographically and its support functions (such as processing, hosting, backup, support and management), divided among suppliers (often across national boundaries) to enhance their data security, disaster recovery and resilience. In this regard, this progress in technology towards a 'distributed' network infrastructure challenges traditional data and outsourcing concepts such as the physical data localisation and auditing of physical premises.

According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. There is a need to harmonize EU financial supervisors' criteria when approving cloud projects

Prescriptive regulations on data localisation are at odds with trends in technology. The latter, unlimited by geographic boundariescan manage storage and access to data, located globally.

We observe that several EU countries[1] have introduced, at national level, additional limitations and barriers which prevent data circulation and intra-group synergies at EU and international level. These have an impact on risk management, centralised/shared infrastructure strategies, and the ability to provide products and services to global customers.

Banks need to be able to transfer data across borders efficiently so as to respond to customers' needs: delivering goods and services, processing payments or providing customer support. To achieve cross-border data flows, there must be no direct or indirect restrictions on data localisation. Limiting data flows without objective and justified reasons undermines the ability of companies to define their business models; it will be detrimental to competitiveness and growth of EU companies; and, endanger the functioning of critical infrastructure.

We would argue that whilst Member States' interests in national security and law enforcement are fully legitimate in most cases (not least those linked to non-personal data), there is no valid justification for data localisation. In practice, these interests are too often used to justify, largely unrelated, measures. We agree with the Commission's statement that localisation restrictions rarely advance the public policy objectives they are intended to achieve.

The EBF fully supports any EU initiative that could remove restrictions to the free flow of data which at the same time acknowledges the right that businesses have to choose where they store their own data. Companies'decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a legislation obligation to do so. At this stage, we consider appropriate the two steps the European Commission intends to take: assessment of the situation (discussion on justification and proportionality of data localisation measures) and, depending on the findings of this assessment, addressing the issues (potential infringement proceedings).

2. ACCESS TO AND RE-USE OF NON-PERSONAL DATA

Data issues is a key commercial and strategic business decision for a company. Data have a strategic value for entities and this value is fundamental to being able to compete fairly in Digital Markets and in the Data Economy.

The data under consideration in section 2 of the consultation are non-personal data (and especially machine-generated data).

[1] As an example, under Article 38 of the Austria Banking Act, credit institutions (banks included), their members, members of their governing bodies, their employees as well as any other persons acting on behalf of these credit institutions must not divulge or exploit secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers, or on the basis of Article 75 para. 3 (banking secrecy. The obligation to maintain secrecy applies for an indefinite period of time. A credit institution may not invoke its banking secrecy obligations in cases where the disclosure of secrets is necessary in order to determine the credit institution's own tax liabilities. These provisions also apply to financial institutions and contract insurance undertakings. This provision is applicable to natural and legal persons either way, and must be respected within a group as well, as – within a banking group – every credit institution is bound to its observance.

It is not clear, at this stage, that banks would have a commercial or financial interest in trading non-personal data. In our view, the intention of the European Commission to address the issue in contracts (data usage licenses) is a good option. Guidance on how to avoid misuse of data would be welcome.

Importantly, the sharing of non-personal data with other operators for the banking sector needs to be **voluntary** and **according to a price or a negotiating contract**. According to their business strategy/model, companies need to be able to leverage the data value in the market and, furthermore, be able to protect and avoid sharing the data that they want to keep safe, or which is only for internal proposes.

Besides the costs and value of data, there are opportunity costs and risks (i.e. regulatory compliance) and cyber risk issues that should be considered. Therefore we think non-personal data owned by financial companies may be shared against payment but always on a voluntary basis.

3. LIABILITY FOR PRODUCTS AND SERVICES COMING OUT OF INTERNET OF THINGS (IOT) TECHNOLOGIES AND AUTONOMOUS SYSTEMS.

Currently, the banking industry does not offer products and services coming out of the Internet of Things (IoT), but might explore these options in the future in case the banking business models becomes broader. Sensors will most likely be used on the insurance side to define risk profiles and pricing conditions. In this case, liability for failure would have a limited scope.

This said, it is fundamental that each actor assumes his/her own responsibility in the process. Accountability scope should be clearly established.

4. PORTABILITY OF NON-PERSONAL DATA, INTEROPERABILITY AND STANDARDS

It is not clear, at this stage, whether the banking sector would have a commercial or financial interest in trading non-personal data. Banks are users of cloud services and view the European Commission's commitment to support the appropriate standards to improve interoperability, portability and security of cloud service, positively

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp
Senior adviser Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69