Consultation of European Supervisory Authorities

17 March 2017

EBF_025978A

EUROPEAN BANKING FEDERATION'S COMMENTS TO THE JOINT COMMITTEE DISCUSSION PAPER ON THE USE OF BIG DATA BY FINANCIAL INSTITUTIONS

(JC- 2016-86)

Key points:

- Data are at the centre of the digital revolution and consequently the use of data analytics is creating increasingly 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 businesses. Data analytics contribute widely to a better internal understanding of the banks' activities, a more effective risk management, and an improved monitoring of compliance. They can also contribute to building a stimulating customer experience.
- When defining or describing the big data phenomenon we should bear in mind that it is a cross sector phenomenon. Indeed, companies from other sectors (e.g. energy, telecommunications, and pure digital giants like the GAFAS (Google Apple Facebook Amazon) make use of big data. So do other less regulated players like Fintechs start-ups. Thus a sector specific approach should be avoided as well as regulatory instruments only applicable to the financial sector. The principle "same services/risks, same rules" should apply to all companies regardless of the sector or location. The focus needs to be on assessing the activities rather than the institutions that offer them.

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

- Considering that further evolutions of the phenomenon are expected to emerge in the use of Big Data, the banking sector is currently assessing the applicability of Big Data and the deployment of technological developments as well as the impact of existing and recent legislations on the innovation. Indeed, several existing EU legislations and/or other regulatory requirements already apply to Big Data such as the Payment Services Directive 2, the General Data Protection Regulation (GDPR), the Markets in Financial Instruments Directive (MIFID 2), etc. (even if they do not make an explicit reference to it). They already mitigate potential risks. The EBF encourages the ESAs to continue monitoring the market and the impact on the digital environment of existing and recent legislations before considering further steps.
- The EBF welcomes the opportunity to comment on the ESAs consultation and strongly encourages continuous dialogue between stakeholders and the policy makers, regulators, supervisors and the competent authorities such as the Article 29 Data Protection Working Party (future European Data Protection Board) to ensure the legislative framework is adjusted to the digital reality.

EBF RESPONSES

1. Do you agree with the above description of the Big Data phenomenon? If not, please explain why. Please also mention whether you consider that other characteristics are relevant to understanding the use of Big Data.

We generally agree with the description of "Big Data phenomenon" provided by the European Supervisory Authorities (ESAs) mentioning that big data corresponds to the collection, processing and use of high volumes of different types of data from various sources, often using powerful IT tools and algorithms.

However, although big data is not yet mature in all industries tackled by the consultation, it should be highlighted that some of the elements included by the ESAs in the definition correspond to a phenomenon applied for a number of years now. For example, concerning volume, card processors have always used a vast amount of data. Relating to variety, banks have traditionally been combining their own data with credit bureaus' in order to assess the customers' ability to repay loans, resulting from a combination of data to which banks have access to, rather than necessarily accessing new data.

Further consideration should also be given to the approach undertaken by the companies in their use of data and the impact of technological developments:

- it is interesting to note that when using data many banks start from a business position/goal and then assess what data is required in order to achieve that goal;
- in recent years, computational power has increased, due to the development of the Cloud and the Internet of Things (IoT).

In addition, particular emphasis should be given to the verification of the dataset: controls across the data flow to assess data against the accuracy, reliability, completeness and timeliness criteria defined in the data policy and associated standards.

We believe it is very difficult to establish a clear definition of "Big Data" as it would change along the years. Establishing a limitative definition in a regulatory instrument that is only applicable to the financial sector should be discouraged. Indeed, companies from other sectors (e.g. energy, telecommunications, and digital giants like the GAFAs (Google Apple Facebook Amazon)) make use of big data in an even more intensive way than financial institutions, so do other less regulated players like Fintech start-ups. When defining or describing the big data phenomenon we should bear in mind that it is a cross sector phenomenon, thus, avoiding regulatory instruments only applicable to the financial sector.

For the sake of simplicity, we will be using the wording of "Big Data" within our comments on this discussion paper.

2. Which financial products/activities are (likely to be) the most impacted by the use of Big Data and which type of entities (e.g. large, small, traditional financial institutions, Fintechs, etc.) are making more use of Big Data technologies? In light of ESAs' objective to contribute to the stability and effectiveness of the financial system, to prevent regulatory arbitrage, do you consider that there is a level playing field between financial institutions using Big Data processes and those not using them (e.g. because they do not have access to data or the (IT) resources needed to implement Big Data processes) or between established financial institutions and potential new entrants (e.g. Fintechs) using Big Data processes? Please explain.

1. Products and activities concerned

It is important to note that customer data has been at the heart of the banking business model for a long time and affects every level of banking activity such as corporate/investment banking, retail banking, credit management and analysis/ mortgage, transfer operations, payments, cash management, risk management and compliance, cybersecurity as well as IT departments etc.

Any kind of financial product/activity is being impacted and particularly those that are virtualised/digitalised, with priority to the application of predictive models to marketing (cross selling and pricing), to processes (optimisations, prioritisations, operational strategies), risk management (early warning systems, rare events) and security notably based on legal requirements.

2. Types of entities

Nearly all financial institutions are likely to be impacted by the use of Big Data, the insurance sector in particular but also banking. Any kind of financial institution can take advantage of Big Data. For example, a large organisation for which Big Data is already a reality and smaller ones such as a Fintech start-ups, as their business model is often based on their capabilities to analyse large volumes of data including Big Data. Even if Big Data is initially not part of a financial institution's main business model compared to tech giants, it will have an impact owing to the increasing competition, mainly from companies which are not banks and which now offer financial products.

For the big challenge going forward the emphasis lies less on technology than on finding the right people and the costs of governance. The huge amount of legislation and compliance limit companies' investment capacity to use big data. In addition, (a part of) society may still be sceptical as to the added value of big data for the individuals. Thus another challenge for banks lies in making clients aware of the added value of the analysis of their (small or big) data for them.

Cloud adoption along with the emergence of more packaged solutions like the use of semantic technologies on top of Big Data tools like Hadoop HDFS and Apache Spark (smart data lakes) and the accompanying democratization of data access will open up Big Data opportunities to small and medium sized banks. We observe already that cloud services and open source software, crucial for Big Data processes, are accessible to entities of all size. This is proved by the appearance of Fintech start-ups whose business model is based on the analysis of data (such as account aggregators) and are quite successful while being, at the same time, low capitalised companies.

Big Data also affects bank's customer centric strategy as it helps banks to explore improvements in the speed of customer communications in an environment with growing expectations of immediate response interactions.

3. Level playing field

a) Level playing fields between financial institutions using big data processes and those not using them

There is a difference between financial institutions competing in global markets and those competing in a local market. A local bank with a few thousands of customers would probably only need limited good analytics in addition to the knowledge of its local customers compared to big banks active on a global market. The development and implementation of Big Data solutions concerns considerable investments, irrespective of the size of the institution.

It is worth noting that there is a substantial difference in the value proposition of players that adopt Big Data technologies compared to those who do not, pushing each and every entity to adapt to the new digital reality, including adopting Big Data to respond to the competitive environment and the new customers' expectations.

b) Level playing field between established financial institutions and potential new entrants (e.g non-banks Fintech) using big data processes

As part of a general approach to the banking transformation, banks engage more and more in Fintech partnerships, and finance innovative starts-ups. Some banks have already developed Fintech accelerating platforms, Fintech labs to focus their activities even more on customer experience and to help them to deal with the new generation of customers. Fintechs have a role to play in speeding up the industry and they can be used to improve the business model. Fintechs can create many opportunities for banks such as helping them to improve their business model, cut costs and build activities which are complementary to banking activities conducted in-house.

- A regulatory discrepancy between banks and other types of actors remain an important barrier that prevents financial institutions from using consumer data in a beneficial way. It is worth highlighting that the number and diversity of actors to be considered in this new scenario includes not only Fintech start-ups, but also tech-giants.

  Those entities have gained a dominant position in a specific market (e.g. search engines or social networks) which allows them to collect impressive amounts of data. These companies could use such Big Data in order to access different markets, using their position in their market of origin to strengthen their presence in new sectors such as the financial market, putting financial institutions to a competitive disadvantage and not always setting priority to the data subject interests. In some countries, there are, currently, non-financial services providers entering the digital market that provide similar financial services despite not being subject to the same regulation as financial entities, and are thus not playing under the same rules (this is particularly true for PSD 2). Moreover, they are not subject to the strict supervision of the financial authorities and the requirements for previous authorizations that are relevant for banks.

- At the same time we observe that Fintech start-ups have usually a short-term approach focusing only on the customer experience and less on risks, compared to banks which have a long-term one with further consideration for the risks and reputation.

Policy-makers should adopt a holistic approach and ensure that EU regulation is adjusted to the digital reality for financial services as well. The focus needs to be on assessing the activities rather than the institutions that offer them. This is not a call for new regulations but rather for adjusting, simplifying, removing obstacles and inconsistencies and modernising the EU regulatory framework as well as making sure that new players on the market do also consider the interests of the data subjects. It is fundamental to have an appropriate competitive environment with a level playing field among all the different players which would ensure wide-ranging high standards and, in turn, enhance consumer trust. It is also in the interest of the data subject/customer that s/he may rely on the fact that all players in the market, regulated or not, bank or non-bank treat his/her data with the same care and that the same legal framework applies.

Moreover, if such an environment is not ensured then banks will not be able to compete on an equal footing in the new digital era where data is the driver of business (e.g right of data portability).

3. Do you offer/are you considering using Big Data tools as part of your business model? If so, please briefly describe: i) what type of entity you are, e.g., long established, start-up, a product provider, an intermediary; ii) the service you provide; iii) the nature of your clients; iv) your business model; v) whether the Big Data tools/strategy were developed by an external company or internally and whether you have related agreements with other entities (including non-financial entities); vi) what are the types of data used (personal, anonymised, user data, statistical data etc.) sources of data; and vii) the size of your Big Data related activity and/or forecast activity (e.g. to what extent are business decisions already taken on the basis of Big Data analysis; what other business actions could be based on Big Data in the future)?

i) Description of the entity

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 2.5 million people of which large part have experience with innovative uses of consumer data in their daily activities. The EBF members represent banks that make available loans to the European economy in excess of €20 trillion and securely handle more than 300 million payment transactions per day.
As a result, the response to the discussion paper is therefore provided in the capacity of a long-established financial institution representing the banking sector which aims notably at developing innovative products and the best products and services for its customers.

ii) Services provided

EBF's Member's banks provide their customers with a wide range of financial products and services covering different business needs (Corporate, Retail and Financial Institutions) and "vertical" area of business (insurance, wealth management etc.).

iii) Nature of the clients

EBF's Member's banks provide all kind of financial services for any kind of customer, from individuals to the largest national firms, government institutions and multinational companies.

iv) Business model

EBF's Member's banks business model is based on covering their customers' needs by a multichannel and multi product/service organization

v) Development of the big data strategy

The majority of banks have established a dedicated internal team that deals with the development of Big Data projects to support the entire group. Banks are also supported by external partners – and Fintech start-ups are among them – which provide them with the best knowledge transferred to specialists.

As part of a general approach to the banking transformation, banks engage more and more in Fintech partnerships, and finance innovative starts-ups. Banks have already developed Fintech accelerating platforms, Fintech labs to focus their activities even more on customer experience and to help them to deal with the new generation of customers.

vi) Types and sources of data used

Types of data used

The type of consumer data that financial institutions most commonly use are:

- **Identity and demographic data** (e.g. ID, age nationality, address, education, professional details);
- **Credit history** (e.g. history of credit use);
- **Transactional data** (e.g payment account movement (credit and debits));
- **Payment obligations** (e.g. to evaluate the debt service ratio and the remaining net income);
- **Behavioural performance data** (e.g. credit incidents, debt falling due, potential debt)
- **Perception of the financial institution's service level** (e.g. customer expectations and satisfaction/complaints);
- **Use of channels** (Web, Mobile, Phone, Branch)

It is also important to note that financial institutions use the data listed, in the context of being able to provide their services to their customers, risk management, fraud management, product management, customer service, reporting to supervisors, marketing, etc.), notably to comply with legal obligations.

There are indeed areas in which financial regulators require banks to perform specific accuracy tests which do not fully rely on the data that customers or the market participants provide. Rather, banks also rely on high quality data that corresponds to "managed/derived data", data which has undergone a thorough process and analysis conducted by banks (such as verification, cybersecurity, etc.) in order to be used.
This kind of data is not necessarily identifiable to individuals. It leads to an enhancement of raw data and to the creation of new data as part of the intellectual property of banks. These processes create an additional layer of value from the raw data.

In this sense, it would be advisable to differentiate between raw data (provided directly by the customer) and managed/derived data (data which has undergone a thorough process and analysis conducted by banks (such as verification, cybersecurity, etc.).

Some companies, mainly banks, tend to enhance the quality of the raw data they receive from customers and other sources. In fact, they 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.

We believe it is important to recognize that there is an added value in the data managed by those companies. When the customer applies for data portability, we believe that this should only include the raw data that he/she has provided, but not the data of enhanced quality that is the result of further verifications and analysis run by the data controller to fulfill his/her legal obligations.

Sources of data used

The large majority of data processed by banks are used for conventional purposes such as processing transactions on customer instructions, regulatory compliance (e.g. Know Your Customer (KYC) and Fair Treatment of customers' requirements in certain countries, Markets in Financial Instruments Directive (MiFID), prevention of fraud (e.g. using mobile localisation), money laundering/terrorist financing and other financial crime, and credit worthiness assessment requirements) as well as the data used for marketing purposes.

Data made publicly available by consumers could represent a complementary source for banks provided that it is used in line with data protection legislation. It is not known yet whether this will be used structurally in the future but its possible value should not be underestimated or overly valued.

The main sources of consumer data that financial institutions rely on are both internal and external data:

- **Data directly provided by the customer** based on:
  - the consumer's informed consent (when required and which include customer feedback and data collected via satisfaction surveys in order to improve the customer relationship or filling in forms prior to entering into a contractual relationship with the bank);
  - legitimate interests (legal requirements, AML requirements etc.);
  - the processing is necessary for the performance of a contract to which the customer is party or in order to take steps at the request of the customer prior to entering into a contract or due to compliance with legal obligation.
- **Data produced by bank operating systems;**
- **As a complementary tool, external data such as public and/or private managed specialised databases** (e.g. from the incident credit records/ National Database on Household Credit Repayment Incidents/ credit bureaus to conduct the creditworthiness assessment), information originated from the client's financial turnover, transaction patterns and preferred products/services statistical data, publicly available data, credit rating agencies, Politically Exposed Persons (PEPs) lists, governmental statistics offices, etc.).

vii) Size of Big Data related activity and/or forecast activity (e.g. to what extent are business decisions already taken on the basis of Big Data analysis; what other business actions could be based on Big Data in the future)

Consumer data, including Big Data analytics is used today in particular to:

a) Improve the customer experience and satisfy customer needs :

The data collected (based on customers' consent when required) facilitate the understanding of customers' needs, the quality of products and services provided and contribute to the development of personalised offers in real time; Consumers will, for instance, be able to benefit from more individualised offers for loan rates or a simplified and faster approval of their loan's request due to a better assessment of the risk profile.

The assessment, evaluation and interrogation of transaction information and the detailed analysis of this can provide a more detailed insight into customer behaviour identifying specific needs, issues and areas on which a customer may require assistance. This can support a more targeted marketing campaign or simply advance a customer relationship with the bank.

b) Comply with legal and regulatory requirements and risk management:

- The collection of personal data and its analysis is moreover necessary for profiling for risk management, creditworthiness assessment purposes and/or financial crime prevention. For example, fine-tuning the parameters used in fraud monitoring systems to improve their ability to detect and prevent related fraud, as requested by financial services requirements. These procedures are widely recognised as being the most effective and fair (if not the only possible) way of assimilating data in order to make responsible financial decisions.

  Their use derives from legal requirements in various EU and national laws such as the new Anti-Money Laundering Directive (AMLD[1] – which imposes a customer due diligence and Know Your Customer requirements and is considered as awful way of processing according to the new General Data Protection Regulation), Markets in Financial Instruments Directive (MiFID)[2], the Consumer Credit Directive (CDD)[3] and

[1] *Article 13(1)(a) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC provides that Customer due diligence measures shall comprise: identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.*

[2] *Article 13(5) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC provides that (…) An investment firm shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.*

[3] *Article 8 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April on credit agreements for consumers and repealing Council Directive 87/102/EEC provides that Member States shall ensure that, before the conclusion of the credit agreement, the creditor assesses the consumer's creditworthiness on the basis of sufficient information, where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant database.*

the newly adopted Mortgage Credit Directive (MCD)[4]. The use of consumer data therefore also contributes to lower the credit risk and thus to the resilience of the European banking system. It is worthwhile noting that this is especially true for risk dependencies, which constitute a major source of systemic risk so intensively discussed in the context of macroprudential supervision over the last year, and which can finally be effectively managed for the first time through the use of big data analytics.

It is also important to note that the recent European Commission's proposal amending the 4th AML Directive, published on 5 July 2016, might impose on banks additional requirements regarding the collection of data to address terrorist financing risks linked to high-risk third countries.

Enhanced measures will lead to extra checks and monitoring of those transactions by banks and obliged entities in order to prevent, detect and disrupt suspicious transactions involving "high risk third countries". A Communication and a proposal amending the Directive on Administrative Cooperation in the field of taxation were also published to tackle tax evasion and tax avoidance in the EU. According to the Commission, tax authorities should have access to national anti-money laundering information, particularly beneficial ownership and due diligence information and new, accounts should be subject to due diligence controls.

Those recent initiatives strengthen the requirements imposed on banks to collect consumer data.

c) Contribute to the business performance of banks, banking techniques and create new business opportunities.

Consumer data is used in the context of customer satisfaction surveys which allow banks to improve the services they provide for their customers, for process optimisations purposes as well as for the development of new innovative tools such as automated financial advice. The innovative use of consumer data represents an advantage which allows banks to run their business more efficiently and at a lower cost, develop a faster decision-making process and improve their customer segmentation activity.

---

[4] *Article 18 of Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 concerning the obligation to assess the creditworthiness of the consumer provides:*
1. Member States shall ensure that, before concluding a credit agreement, the creditor makes a thorough assessment of the consumer's creditworthiness. That assessment shall take appropriate account of factors relevant to verifying the prospect of the consumer to meet his obligations under the credit agreement.
2. Member States shall ensure that the procedures and information on which the assessment is based are established, documented and maintained.
[…] 5. Member States shall ensure that:
(a) the creditor only makes the credit available to the consumer where the result of the creditworthiness assessment indicates that the obligations resulting from the credit agreement are likely to be met in the manner required under that agreement;
(b)in accordance with Article 10 of Directive 95/46/EC, the creditor informs the consumer in advance that a database is to be consulted;
(c) where the credit application is rejected the creditor informs the consumer without delay of the rejection and, where applicable, that the decision is based on automated processing of data. Where the rejection is based on the result of the database consultation, the creditor shall inform the consumer of the result of such consultation and of the particulars of the database consulted.
6. Member States shall ensure that the consumer's creditworthiness is re-assessed on the basis of updated information before any significant increase in the total amount of credit is granted after the conclusion of the credit agreement unless such additional credit was envisaged and included in the original creditworthiness assessment.
7. This Article shall be without prejudice to Directive 95/46/EC.

It also enables banks to reduce inappropriate marketing expenditure, avoid the development of unnecessary product and services offerings, and focus more effectively on their capacity to innovate for the benefit of their customers.

Profiling to support the development of 'tailor-made' products or services for customers is therefore a crucial tool for financial institutions. It is also used for risk assessments for preventing fraud and money-laundering which, in this case, is mandatory.

Thus, the processing of consumer data is lawful because it is based on different legitimate purposes as: preventing criminal actions, building consumers' trust in the digital economy as well as developing e-commerce.

There is also an increasing interest in the provision of new non-financial products based on the knowledge derived from banks'' activities which could help customers make better decisions. While developing these products financial institutions allow customers to strike the balance which has to be achieved between access to innovative products tailored to the needs of customers, and protection of their privacy.

Other business actions to be undertaken in the future

The use of 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 creating increasingly 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.

Given the changes in society and the use of social media, the new generations of customers might arrive with fresh expectations. They might expect banks to take into account the data, already at their disposal, when offering services (in respect of the data protection legislation). Importantly, consumers expect banks to be able to deal with financial data in a highly confidential and trustworthy manner.

The future performance of the financial industry will very much depend on the ability of financial institutions to use their customers' data and the interaction of that data with banks' products and services, and, more importantly, to maintain the existing level of customer trust. Data analytics, should contribute positively to maintaining trust, transparency, and security.

a) Increased fraud detection and prevention:

As for authentication and fraud monitoring processes we believe that customer behaviour analysis will become more important and therefore customer data will play a key role in fighting against cybercrime and terrorism financing.

b) Better service for consumers:

In the coming years, more and more useful data analytics 'methods will be developed and used to interpret a vast amount of data.

This will further improve the product and service offering of financial institutions to their consumer and business clients (e.g. real time offers, more innovative and tailored-services, faster credit assessment) and providing a full picture of consumers' needs via different channels (e.g. customers can access the latest information, whatever the channel chosen, and with a single click a customer can access all the accounts he/she holds in a bank).

The focus will be even more on customer relationship management (CRM) and personal finance management in order to help the consumer manage their finance on a daily basis. It might also help in the long term to increase the benefits of banking services and facilitate financial inclusion.

c) Increased business performance and innovative solutions:

With the use of consumer data banks will be able to improve their business performance and develop more innovative solutions which includes a faster decision-making process and improve their customer segmentation activity.

d) Increased transparency in the use of consumer data by certain institutions:

In the field of payments, in line with the PSD 2 and with the view to protect customers, Third Parties Providers (TPPs) should not have access to more data that the data required to either initiate a payment or aggregate payment accounts. In case of payment initiation, TPPs should not be given access to all payment data as it is the case today with screen-scraping. This practice should be banned as it goes well beyond what is necessary to initiate a payment. Equally, account aggregators should only access the data to which consumers have agreed to. In line with the EBF's suggestion[5] to make full use of the provisions of the eIDAS Regulation, the EBA has, in its draft RTS, proposed that TPPs rely on qualified certificates for electronic seals for the purpose of their identification towards all stakeholders.

e) Use of innovative and non-traditional banking tools:

Some banks might also experiment with location-based services (LBS) in an attempt to personalise customer products and services and tighten security for example for mobile transactions. Several banks have launched a mobile-Point-of-Sale solution, known as mPoS, which allows businesses and self-employed professionals to accept card payments using a smartphone. Other banks have built online communities of merchants using a PoS terminal which allows cardholders to access offers and promotions using geolocation technology.

f) Interdisciplinary data usage:

Today, some banks may still be working with partly decentralised or fragmented systems via departmental silos. This does not allow banks to share and benefit from internal data across the organisation contrary to other companies. Consequently, banks will fully adapt their infrastructure and IT systems according to the expectations of data-driven customers taking into account possible applicable legal and compliance restrictions. It will also result in a more efficient data storage and data processing.

g) Further consideration to data protection and security:

Data protection and security have always been key concerns for banks, which use the data that consumers provide for them in a secure way and intend to keep it that way. Confidence in banks as trusted parties is essential for their reputation and adds to the efforts and investments put into maintaining and improving setups ensuring the safety of

5 *See EBF submission on the EBA Consultation Paper on the draft RTS on strong customer authentication and common and secure communication under PSD2*

customer data. Banks have always been respectful of provisions on business confidentiality. For instance, numerous European Banking laws clearly state that banks are subject to professional secrecy. In that context banks are likely to turn data security and protection into a competitive advantage in the years to come.

h) Increasing partnerships with Fintech companies and other industries to respond to customer's needs:

As expressed above, as part of a general approach to the banking transformation, banks engage more and more in Fintech partnerships, and finance innovative starts-ups.

Banks have already developed Fintech accelerating platforms, Fintech labs to focus their activities even more on customer experience and to help them to deal with the new generation of customers. Fintechs have a role to play in speeding up the industry and they can be used to improve the business model. Fintechs can create many opportunities for banks such as helping them to improve their business model, cut costs and build activities which are complementary to banking activities conducted in-house.

In addition, banks might partner with other industries, such as the manufacturing industry and the health industry, in order to develop new products and services.

4. If you are a consumer or a consumer organisation, do you witness any of the uses of Big Data? In what fields?

/

5. Do you consider there are (non-regulatory) barriers preventing you (or which could prevent you in the future) from collecting and processing data? Are there barriers preventing you from offering/developing Big Data tools in the banking, insurance and securities sectors? If so, which barriers?

Generally speaking, we consider there are some non-regulatory barriers that could prevent a financial institution from collecting and processing data.

- **Ability to adapt and change legacy technology and keeping pace of the changing technical landscape**

Technological barriers could (potentially) emerge.

Financial institutions might face difficulties in upholding their competitiveness, responding to innovative needs and at the same time ensuring that their technologies are adapted to new compliance requirements. Banks run critical infrastructures and are therefore subject to additional prudential requirements that incurs higher cost for maintaining and adapting the systems to the changing technical landscape. If technological obstacles are to be overcome, financial institutions could be forced to limit the use of Big Data which would be detrimental for their customers.

Big Data applications involve data processing, complex Big Data analysis modeling and quick extraction of core and effective information. These applications require highly qualified employees (e.g. data strategists, engineers, statisticians, data analysts) who need to develop specific analytical skills to deal with complex Big Data management systems. The lack of employees with the appropriate skill-set, is the biggest barrier to the development of Big Data tools in the banking sector. To respond to this challenge banks are developing a training programme that involves the Data Owners, Data Technical

Owners and Data Scientists and, at the same time, banks are recruiting talented young professionals for Data Science positions.

- **Reputational risk with regard to use of consumer data**

Confidence in banks as trusted parties is essential for their reputation, a fact which adds to the efforts and investments put into maintaining and improving setups ensuring the safety of customer data.

The future performance of the financial industry will very much depend on the ability of financial institutions to use customer data, the interaction of that data with banks' products and services, and most importantly, the ability of banks to maintain the existing level of consumer trust.

Customers trust banks with their data. Banks are indeed the type of company that are the most trusted to manage customer's data securely according to recent studies[6]. However, even if the traditional role of lending, deposits or distribution of currency will continue to be part of the bank business model, it is by no means sufficient to enable banks to remain competitive. The role of banks should not be limited to just providing traditional banking services and providing only secure infrastructure for other players nor, leaving it to others to address the changing customer demands. We observe that consumers' expectations toward financial institutions are completely different compared to non-financial players which have built their business model on data. Banks should be allowed to go further and anticipate customer expectations and/or provide a broader value proposition to customers while keeping trust, security and customer experience at the centre of their strategy. To this aim further awareness should be brought to the benefit of big data analytics notably by public authorities and the industry.

It is important to refer to the reputational risks they could face in case of non-compliance with legal requirements, for example anti-money laundering requirements subject to important fines or a failure to their IT system due to cyber-attacks.

- **Cost and capacity constraints**

Most banks face budgetary constraints at a moment when European banks' profitability is under stress due to the low interest rates environment. This situation coexists with a challenging calendar for regulatory implementation which will have a critical impact on the competitive landscape (MIFID II, PRIIPs, PSD 2 due to enter into force by 2018, at the same time as the General Data Protection Regulation). Banks are already devoting an important part of their resources to regulatory compliance. They should be able to do so without losing sight of their strategic digital transformation.

6. Do you agree with the above short, non-exhaustive, presentation of some of the main applicable requirements? If not, please explain why. Please also mention whether you consider that other legal requirements are essential and should be mentioned.

- We agree with the regulatory requirements identified in this document but would like to emphasize that the requirements identified should not be understood as specific to the financial services sector, on the contrary.

[6] Febelfin study (see graph 8 page 16 in particular:http://files.febelfin.be/Banque_numerique-vie_privee/index.html#16 and https://www.febelfin.be/fr/big-data-au-service-du-client.

Indeed, some of the points raised in the presentation of the main applicable requirements, are presented as being specific to the financial services' sector when those requirements are applicable to any sectors, in particular regarding data protection requirements.
For example, paragraph 24 mentioning that "financial institutions should assess how best to communicate, clear, meaningful, information about data processing, and the use of Big Data tools to consumers", "how individuals may feel if they knew social media content about them was being used" etc. In addition, we are not aware of the situation described by the ESAs that, in addition to the UKs, other data protection bodies have specifically advised financial institutions to consider whether they have legitimate grounds for using data gathered from social media platforms or other online sources [for insurances purposes], rather than merely relying on the fact that some content is accessible.

In principle, banks are careful with the use of data from social networks due to the legal uncertainty around the possible use of this kind of data. Some banks are, however, investigating the potential use of data which are made publicly available by consumers as they could represent a complementary source for banks. Indeed not all (third-party) data sources have the same level of reliability, so banks consistently perform validation processes to ensure its accuracy and may for example decide in the future to cross-verify the information by using public data sources.

In our view, the general data protection rules including the transparency requirements on the use of certain categories of data and the importance to ensure that data are accurate and updated overtime, is fundamental. This is particularly relevant when the use of Big Data has legal consequences on the data subject (e.g. in the creditworthiness assessment). These requirements should prompt the Data Controller to avoid practice such as collecting non authentic data.

- We would also like to emphasize that the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications' sector is under review. On 10 January 2017, the European Commission adopted a proposal for a Regulation on Privacy and Electronic Communications to replace the current Directive.
- Regarding the transparency about data processing, please note that the Article 29 Data Protection Working Party (future European Data Protection Board), announced in its action plan for 2017 that it will start its work with the production of guidelines on the topics of consent and profiling and continue in the second semester of 2017 with the production of guidelines on the issue of transparency.
- Finally, we also suggest considering the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. This is an important new legal framework that might have some impact on Big Data.
- We agree with the importance for financial institutions using big data to be mindful of several consumer protection principles, including the Unfair Commercial Practices Directive (UCPD). It is however important to recall that Article 3(4) and Recital 10 of the UCPD clarify that the UCPD complements other EU legislation that regulate specific aspects of unfair commercial practices. Consequently, where sector-specific or other EU law is in place and its provisions overlap with the provisions of the UCPD, the corresponding provisions of the *lex specialis* prevail. It is important to recall that for financial services, Member States have put in place national rules that provide consumers with safeguards which add to and complement those laid down in the UCPD.

- Regarding the list of rules under "Sectoral Financial requirement" we believe that Big Data can be used to help financial institutions to comply more thoroughly with regulatory requirements.
- Financial supervisor's regulation on outsourcing are also relevant norms to be considered in this context. As many Big Data solutions are based on cloud computing technology, it is important to take into account that the current situation, with a lack of harmonised criteria followed by EU financial supervisors, regarding cloud projects' approval, may be considered as an indirect barrier to big data.
- Although still under discussion, any future policy or regulatory development in relation to the EC Free Data Flow Initiative should be taken into account, as part of the regulatory framework to consider as regards Big Data.

7. Do you consider any of these regulatory requirements as unjustified barriers preventing you from using Big Data technologies? If so, please explain why. Please also explain whether you consider that further regulation (including soft law/guidance, etc. and insofar as it falls within the scope/remit of the ESAs) should be introduced to facilitate the use of Big Data technologies.

We believe that none of the current regulatory requirements described can be considered as unjustified barriers for Big Data technologies. We, however, believe the current banking regulatory environment does not reflect the fast moving digital phenomenon. This is not a call for new regulations as we do not consider that any further regulation (including soft law/guidance, etc.) should be introduced to facilitate the use of Big Data technologies, but rather for adjusting, simplifying, removing obstacles and inconsistencies and modernising the EU regulatory framework. Currently, the regulatory framework does not allow banks to take full advantage of technological innovations, hindering the digital transformation of the industry and obstructing the launch of innovative products and services.

The financial services industry has traditionally been highly regulated with the aim of providing security and protection to the consumer and ensuring financial stability. Those regulatory requirements have been established by authorities in charge of prudential issues, data protection, data security, competition and financial stability.

The financial regulatory framework has become very detailed. It determines not only which activities can be performed by a financial institution, but also the precise steps to be followed, from the design of a product to how customers are contacted and informed (sometimes determining exactly the format of the communications documents as in the case of PRIIPs or PAD rules) or how the sales staff is remunerated. We observe that some recent or on-going EU legislations do not yet properly or fully address the developments made possible by digitalisation, leading to certain contradictions or inconsistencies which could hinder the Digital Single Market from becoming a reality. This is notably the case for example concerning the PSD2 and the GDPR (e.g. this is the case of new consent requirements with the prohibition of tacit consent; the information obligations as regards the processing purposes; or even the right to be forgotten if these are interpreted too strictly by data protection authorities). This is not necessarily to say that these new rules are 'unjustified' as such, but it is important to recognise that there may be trade-offs between tighter controls on the use of data and firms' ability to innovate with data. Ultimately, these rules will need to be implemented in a pragmatic manner that will not unduly impact useful innovation.

- **We note for example, that a (too) strict interpretation of the GDPR could considerably limit the ways financial institutions use data-analytics.**

- **Exchange of data between companies within the same group**:

  Financial institutions often need to process personal data within the group of which they are members in order to achieve aims, such as offering a broader variety of products to the clients, or, efficiently tackling fraud.

  Under the Data Protection Directive, third country transfers between firms are broadly manageable, though not without complications owing to the requirement for appropriate safeguards.

  The GDPR recognises in recital 48 that *"controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."*

  Nevertheless, there will be greater difficulties going forward for two reasons:

  1. The new provisions in the GDPR will make third country transfers more difficult. Under the GDPR, the possibility of making an internal adequacy decision within the firm is no longer possible
     In the absence of an alternative adequacy decision by the European Commission, data controllers will instead have to rely primarily on Standard Contractual Clauses for transfers outside their group. For intra-group transfers, firms will need to rely on either Standard Contractual Clauses or on Binding Corporate Rules (BCRs). However, we note that BCRs currently require 18 months or more to be approved and demand will likely increase under the GDPR.
  2. There is uncertainty over firms' ability to rely even on the safeguards provided for under the GDPR. The EU-U.S. Privacy Shield and Standard Contractual Clauses (SCCs), for example, have an uncertain future, given the striking down of the Safe Harbour adequacy decision in 2015 and a more recent court challenge against SCCs.

  We believe further assessment should be conducted on the barriers that prevent banks from processing or storing data inside and outside the EU (linked to data protection, confidentiality, bank secrecy requirements[7], etc.). Ultimately, there should also be a clear legal basis to share information among jurisdictions at group company level.

  We hope – and expect – that the national competent authorities responsible for GDPR supervision will strike the right balance in this matter.

[7] 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.

- **Profiling rules**

  Regulation frequently takes a negative view of profiling. However, as outlined in the discussion paper, profiling can also provide significant benefits to customers. Profiling should not be societally perceived as necessarily negative.

- **Inconsistencies among local outsourcing regulations**

  Another example of inconsistencies can be seen in the case of EU regulators compelling cloud technology to be compliant with local outsourcing regulations which have not been harmonised and which by definition go against the idea of the cloud (which is meant to be cross-border).

  For the financial sector any data migration to external clouds is subject to the outsourcing framework set by supervisors. This requires informing the supervisor on a case-by-case basis and providing detailed information. The process is not subject to clear rules and the information to be provided depends on each supervisors' criteria, so it becomes very slow and resource consuming. Data localisation barriers also affect the migration of banks to the cloud, as the efficiency and cost of clouds depend on the flexibility banks have to localise data in the most convenient place. Such regulations can contradict the core objective principles of the cloud or lead to further inconsistencies. Competent financial/data protection authorities should find the right balance in this matter.

  Today, GDPR does not guarantee technical interoperability in the portability of data, nor direct communication between data controller, unless it is "technically feasible" (which is a concept yet to be clarified). The latest PSD2 (Payment Services Directive) will grant standardised access to payments accounts to third-party providers acting on behalf of a client. A possibility of a reciprocal access to personal data held in other digital platforms in a direct, standardised and automated format, if consented by the data subject, should be assessed for banks. It would allow them to build better products and services for their customers, based on more accurate information about their needs and preferences.

- We also observe that in certain cases national regulators have restricted the use of particular datasets on the basis that it would be an infringement of the rights of an individual. For example a current Irish position prohibits the examination of specific transactional information and requires that this type of information bereviewed on an aggregated basis. For example, the total amount of credit and debits to an account rather than the assessment of the specific transactions themselves. This position is restrictive in fully understanding customers and their needs.
  Even if the GDPR provides further harmonization among national legislations, currently, some national supervisory authorities impose different requirements.

- **Unintended consequences of prudential requirements on the digital developments**

  The prudential regulation has some unintended consequences for the deployment of Big Data technologies in the financial sector: first, it penalises the investment in software by considering it as an intangible asset and deducting it from the computation of CET1 (including any software developed to deploy data techniques). Second, it sets up a framework for remunerations that affects experts on data technologies and does not allow banks to compete with non-financial providers, able to offer equity-like packages, typical of the digital space.

- **Further consideration to the impact of recent legislations not yet implemented**

  Some of the regulations described in the Discussion Paper, such as GDPR or PSD 2, are still to be developed and detailed by Guidelines or technical standards. It is first important to take into account the impact of the implementation of such new legislative instruments.

- **Digital transformation should be understood as a whole, seeking the right balance between the drivers of change and the impact on the existing business model**

  Financial regulators are challenged to provide a regulatory framework that balances the promotion of new digital value propositions while ensuring appropriate consumer and investor protection. To avoid serious market distortions and to find the proper balance between benefits and risks, it is imperative to take into account the fact that business models may dramatically shift to totally new forms of interlinking platforms, interacting layers and valued added services. With this in mind, policymakers should adopt a holistic approach and ensure that EU regulation is adjusted to the digital reality for financial services as well. The focus needs to be on assessing activities rather than institutions that offer them. This is not a call for new regulations but rather for adjusting, simplifying, removing obstacles and inconsistencies and modernising the EU regulatory framework. The current banking regulatory environment does not reflect the fast moving digital phenomenon. New access methods fostering a real cross-border and cross-sector economy (e-ID, e-signature, e-invoicing, online platforms, etc.) may change the way business operates across different markets. This complete shift of paradigm requires a renewed approach in order to balance benefits, risks and avoid market distortions efficiently. Banking legislation needs to be adapted to the digital market reality.

- **The principle of "same services/risks, same rules" should apply to all companies regardless of the sector or location**

  A regulatory discrepancy between banks and other type of actors is an important barrier that prevents financial institutions from using consumer data in a beneficial way. Banks are currently subject to many regulations, which do not apply to non-banks digital financial services providers. There are, currently, non-financial services providers entering the digital market that provide similar financial services despite not being subject to the same regulation as financial entities, and thus they are not playing under the same rules. This is particularly true for PSD 2. The principle "same services/risks, same rules" should apply to all companies regardless of the sector or location.

As a potential solution to assess the impact of data analytics, we believe the supervisors can help the data driven innovations to be deployed across the financial sector by creating a framework of experimentation/regulatory sandboxes as safe spaces where regulated and non-regulated actors can test innovations in a controlled environment. This will also help supervisors to have access to innovative initiatives and assess them after seeing how they work. However, at the same time, it will be important for supervisors to ensure a strong protection of consumers/data subjects when experimenting regulatory sandboxes. In addition, European Supervisory Authorities can play an invaluable role by providing support to national authorities to share experiences and resources and thus making innovation accessible to all countries. This is critical to set up a true European space for financial services.

8. Do you consider the potential benefits for consumers and respectively financial institutions to be accurately described? Have you observed any of them in practice? If so, please provide examples. If not, please explain whether you are aware of any barriers that may prevent the above potential benefits from materialising?

We believe the potential benefits of Big Data usage for consumers and financial institutions described are accurate, in particular, in the ability to personalise products/services, and offer a better customer experience.

However, we believe that there are other potential benefits related to:

- risk management once the product has been sold or the credit has been granted; . using big data tools will allow financial institutions to model their risk more efficiently, manage it, understand and predict its future evolution;
- possibly, an improved credit lending decision which could help ensure that customers do not take on debt they cannot afford; and also lead to an increase in access to credit for customers who are less financially included (non-salaried workforce, limited credit history, etc.); indeed, due to the collection of additional data, customers who have been rejected by financial institutions with existing risk scoring methods due to limited credit history information might benefit from a better access to credit (it is however important to stress that this does not preclude financial institutions from denying access to credit to those who do not meet the required criteria); it could thus bring further certainty for consumers on the possibility of being given a loan and for financial institutions to conduct a more precise creditworthiness assessment.
- in line with improvement of personal finance management, Big Data might also help in the long term to increase the benefits of banking services and facilitate financial inclusion (offer services to those people who rely exclusively on traditional instruments and could be excluded from commercial offerings);
- improve operational efficiency of banks' processes whether it be in the front office or back offices' processes.

This said, it should be born in mind that in order to turn those "potential" benefits into "real benefits", as stressed in the discussion paper (paragraph 64), "new skills, in particular data scientists or behavioural and social specialists will be required to create "new multidisciplinary teams with employees of different background". It should involve an investment from financial institutions but also actions from regulators.

It should be nevertheless clarified that banks are currently exploring the possibilities of Big Data but should not be obliged to "do" Big data. Otherwise a risk will exist that the public will take for granted that Big Data and all its advantages are already being used by all banks, when it may still be under careful consideration

In addition, excessive and burdensome compliance requirements could also represent a barrier to the development of innovations.

9. Do you agree with the description of the risks identified for consumers and respectively financial institutions? Have you observed any of these risks (including other risks that you are aware of) causing detriment to consumers and respectively financial institutions? If so, in what way? If not, please explain why. Please also mention whether certain risks for consumers and financial institutions have not manifested yet but have the potential of developing in the future and hence need to be closely monitored by Supervisory Authorities.

We generally agree with the description provided but believe that the risks outlined are not exclusive to Big Data and some clarifications should be added regarding certain points. Indeed, some risks highlighted do not derive from the use of Big Data but from the use of IT systems (e.g. cyber risk). Please see our comments regarding regulatory barriers (response to question 7).

- Data management becomes a lot more complicated in the Age of Big Data, so we believe that there is merit in the European Commission's ongoing examination of the 'Data Economy'. These issues are complex, so it is important that they be carefully considered in order to avoid potential unforeseen consequences.
- In line with paragraph 55 referring to the risk of "opacity around the provision of services using Big Data could make difficult to challenge the criteria used in the developments of algorithms, the poor quality, the accuracy or the relevance of the data used by firms' analytics algorithms", we would like to emphasize the importance of ensuring that the data processed are reliable. Indeed several risks (financial, ethical, personal etc.) exist which could be generated not only by Big Data itself, but also by the complexity of the ecosystem (open network, applications collecting and processing more and more data). The risks of underlying data and models used to make decisions being inaccurate is quite high and data quality check processes must be continuously enforced and updated. Nonetheless, when building a model, banks carefully assess and take into consideration the quality of the data before it is used (notably in line with strict regulatory provisions imposed on the banking sector).
- Concerning the risks related to access to financial services because of granular segmentation (paragraph 38): considering the changes that big data could introduce into customer segmentation compared to traditional techniques, we do not agree with the conclusion that algorithms could more easily forget outliers. This could happen more frequently when the analyst uses traditional tools, as the results will tend to be less granular. When new datasets are used and artificial intelligence is applied, the result is that new relationships arise and financial institutions become more prone to establishing relationships with individuals that are less serviced. A challenge could arise when trying to apply Big Data analytics for customers who are not tech savvy or have minimal footprint in their digital channels. Nevertheless, banks strive to offer adequate services to each category of (prospective) clients, irrespective of their digital footprint. Of course, a lack of availability of digital information may require banks to obtain any relevant missing information directly from the client.
- Regarding paragraph 39, we do not believe that Big Data will generate decisions that are contrary to the financial institutions overarching obligation to treat customers in a fair and non-discriminatory manner. Such behaviour is related more to misconduct than the use of Big Data. Conversely, it can indeed be argued that automated decisions will lead to less misconduct which could be linked to a human factor.

- Regarding paragraph 40 and the risks that "behavioural data could make it easier, in the future for companies to charge different prices/premiums for the same product/service to customer within the same target group (...)", it is important to clarify that the pricing differentiation is not due to discriminatory criteria (i.e. based on sex, religion, ethnicity etc) but due to the fact that different situations should be treated differently. The fact that two customers are offered different prices is due to their dissimilar situations. For example, this is fairer towards customers who deserve better conditions owing to their more appropriate credit behaviour. Furthermore, it can prevent situations such as granting credit to those who be unable to repay and could go through difficult times in the future because of a loan they would have been better not to have taken.

- Regarding the risks related to the reduced comparability of financial services due to increasing personalisation (paragraph 42): it can be observed that in general personalised offering are still more beneficial to consumers than generic ones as they enhance the added value and the consumer experience.
  We also believe that customers would make better decisions if they relied on an amount of well-explained data. It is important to note that tools such as comparison websites or account aggregators, based on Big Data techniques are being developed, to facilitate comparability.

- Regarding the risks linked to limited/unclear information and comprehension of the extent to which the offer/service is tailored to consumers and/or represents a personal recommendation (paragraph 43): while customers making unsuitable decisions potentially represent a risk for any kind of service provided online, it should be considered that this is mitigated by the possibility for the customer to have a permanent access to an operator (via an online chat, mail or telephone) who would provide assistance throughout the process. In some cases, providing automated financial advice might even avoid any potential conflicts of interest due to human intervention. It is also important to stress that in general, for any financial advice, specific legal requirements would have to be met. However, regarding online platforms and websites some of our main concerns remain, such as:

  - the risk for clients to consider and treat as advice other type of services; The risk of confusion could arise from the fact that the customer based its decision on price comparison with limited information or wrongly perceive an information given by the firm as personal advice.

  - receiving advice without realising it is an advice; the client should provide a clear consent and express his understanding before receiving the advice: the risk would be mitigated if the specific service being provided is clearly explained to the client.

- Regarding the risks for consumers derived from more aggressive marketing or cross-selling practices (paragraph 44), it is important to note that the existing Unfair Commercial Practices Directive (UCPD)[8] already sets a common framework against misleading and aggressive practices within the EU. More specifically for financial services, Member States have put in place national rules that provide consumers with safeguards which add to and complement those laid down in the UCPD.

[8] *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance)*

In addition, on 25 May 2016, the Commission adopted an updated version of the 2009 Guidance on the application of the UCPD[9]. The purpose of this document is to facilitate the proper application of the UCPD. It provides guidance on the UCPD's key concepts and provisions and gives practical examples taken from the case-law of the Court of Justice of the European Union and from national courts and administrations. To facilitate enforcement activities and ensure legal certainty, the updated Guidance highlights questions that are common to all Member States. This includes topics such as:

- the interplay between the UCPD and other EU legislation;
- the mounting case-law of the Court of Justice of the European Union and national courts;
- how the UCPD applies to new and emerging business models, especially in the on-line sector.

- Concerning the lack of transparency around the processing of data expressed in paragraph 54 and 57, it is important to stress that providing information to the customer on the usage of his/her data is mandatory and already imposed by Section IV (information to be given to the data subject) and Article 10 (Information in cases of collection of data from the data subject) of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[10]. In addition the recent General Data Protection Regulation (GDPR) is intended to address those risks. In particular via requirements to provide much more detailed information on data processing to customers under Article 13 (and Article 14) in order to ensure that data processing is fair and transparent. The principle of transparency requires, in particular, that any information and communication relating to the processing of those personal data to the data subject should be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Recital 39, Article 12). Furthermore, under article 6 on "lawfulness of processing" and Article 7, the nature and conditions for consent are expanded and strengthened, it should notably be given "unambiguously". Article 6 also tightly limits the re-use of data for incompatible purposes after it has been collected.
  Moreover, it is important to highlight that the majority of financial entities are taking the appropriate steps towards the simplification of the messages included in their contracts and the clarity of the language used in their drafting.

  It is also worth mentioning that the Article 29 Data Protection Working Party (future European Data Protection Board) plans to issue in 2017 some guidelines on the issue of transparency.

[9] *http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf*

[10] *Section IV (information to be given to the data subject), Article 10 (Information in cases of collection of data from the data subject) of the Directive*
Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

- Regarding the potential lower costs related to enhanced risk and credit-worthiness assessment (paragraph 65): Regarding the reduction of costs for financial institutions in general, it is crucial to note that the personalisation of services will require a lot of investment in order to evaluate innovations, new processes and new ways to share, manage, use and protect data, maintain algorithms etc. This is notably the case for automation financial services.
  Cybersecurity costs are also going to increase significantly and will be key to managing a very significant risk for the financial system and consumers. Financial service providers will therefore be less likely to reduce their costs but more likely to change their distribution. Although some costs will be reduced or even disappear, others can increase with data management, storage, protection, innovation, technical tools, remuneration of very specialized profiles, etc.

10. Is the regulatory framework adequately addressing the risks mentioned above? Bearing in mind the constant evolution of technologies/IT developments and that some of the above mentioned regulatory requirements are not specific to the financial services sector (e.g. GDPR), do you think further regulation is needed to preserve the rights of consumers of financial services in a Big Data context? Please explain why.

The issue of Big Data should not be considered with a sector specific approach as it impacts all sectors. The principle "same services/risks, same rules" should apply to all companies regardless of the sector or location. Regulating specifically the financial sector could have a detrimental impact on its competitiveness.

It is also important to keep in mind that legislations recently adopted such as the PSD 2, GDPR, MIFID 2 etc. still need to be implemented and an assessment of their impact on the digital environment will be needed.

In addition, we would like to stress that the current legal framework requires that personal data is accurate and kept up-to-date. Ensuring that data is accurate, that firms are transparent, and that firms meet their overarching obligations to treat customers fairly is the key point. The existing regulatory framework is appropriate, with firms needing to ensure that each use of Big Data technology, analytics, profiling, etc. is compliant with these fundamental rules.

11. Do you agree that Big Data will have implications on the availability and affordability of financial products and services for some consumers? How could regulatory/supervisory authorities assist those consumers having difficulties to access financial services products?

We agree that Big Data will have implications on the availability and affordability of financial products and services for a specific segment of consumers. Sophisticated analytics can substantially improve decision-making, minimise risks and discover valuable insights. Furthermore, Big Data offers the opportunity of building in – house credit models, which enable banks to reduce costs, target the right audiences, recalculate risk portfolios and optimize offerings. Big Data, in general, homogenizes and democratizes decisions and eliminates subjectivity.

It could lead for example to an improved credit lending decision which could help ensure that customers do not take on debt they cannot afford while also leading to an increase in access to credit for customers who are less financially included (non-salaried workforce, limited credit history, etc.);

Indeed, due to the collection of additional data, customers who have been rejected by financial institutions with existing risk scoring methods due to limited credit history information might benefit from a better access to credit (it is however important to stress that this does not preclude financial institutions from denying access to credit to those who do not meet the required criteria).

It will thus bring further certainty for consumers regarding the possibility of being granted a loan and for financial institutions to conduct a more precise creditworthiness assessment (see our response to question 8)

This will not mean however that all customers will have automatic access to the services. It is important to recall that Big Data is neutral in terms of availability and affordability of financial products and services but its value very much depends on the quality of customer's application. Some risks remain (see our response to question 9) and the risk assessment by the sector will prevail. Governments may have to offer incentives to financial institutions to provide products for high-risk segments.

12. Do you believe that Big Data processes may enable financial institutions to predict more accurately (and act accordingly) the behavior of consumers (e.g. predicting which consumers are more likely to shop around, or to lodge a complaint or to accept claims settlement offers) and could therefore compromise the overarching obligations of financial institutions to treat their customers in a fair manner? Please explain your response.

The use of Big Data will not compromise banks obligations to treat consumers fairly.

By applying an effective Big Data Governance framework, financial institutions can assure that information is consistently defined and understood, increase the quality, use and trust of customer data and comply with the regulatory requirements. As described in answer to question 9, comparison websites or aggregators, as well as all the regulatory initiatives that have been set at national and European level to encourage and facilitate switching make this decision easier for customers.

Consequently, Big Data processes may enable financial institutions to treat their customers in a fair manner. See also our response to Question 10.

Indeed, banks are already managing customer complaints and Big Data could be a very effective tool in this area and in a more convenient manner for both parties (lodge a complaint or accepting claim settlement offers).

13. Do you agree that Big Data increases the exposure of financial institutions to cyber risks? If yes, what type of measures has your institution adopted or is going to adopt to prevent such risks? What could supervisory/regulatory authorities do in this area?

The usage of Big Data may not necessarily increase the exposure of financial institutions.

Assets managing, critical information, should be indeed correctly protected regardless the uses a traditional on-line Analytical Processing (OLAP)/on-line transaction processing (OLTP) Database, or a big-data distributed technology based on Hadoop or similar. Big Data should not change the security paradigm.

It is notably observed that it could contribute to better audit capabilities compare to older systems used in the organisation (e.g exploit the audit logs generated by Big Data tools to understand the normal user's behaviour and detect unexpected behaviour that could relate to attacks or suspicious activities).

As for authentication and fraud monitoring processes we believe that customer behaviour analysis will become more important and therefore big data will play a key role to fight against cybercrime and terrorism financing.

It represents also a benefit for Cybersecurity mechanisms such a Security Information Event Management (SIEMs) risk scoring systems.

After a wave of increasingly sophisticated cyberattacks in 2014, targeting all types of organisations, the banking sector is facing attackers which are streamlining and upgrading their techniques rapidly while the sector is trying to fight back at the same speed. These repeated attacks can affect customers' finance and their confidence, and can have severe economic and reputational consequences on the organisation. Banks in Europe and worldwide are taking these threats seriously. Banks invest heavily in IT systems aiming at the highest possible security levels, but cybercriminals exploit any vulnerability – including on the clients' side to penetrate the system.

Data governance is put in place by banks according to risk profile of customers, as well as appropriate security measures in line with related services or products characteristics, in line with regulatory requirements.

In addition, dedicated regional and global groups have been created, to share information about security threats, for instance, the EU-Financial Services Information Sharing and Analysis Center (EU FS ISAC), and FS-ISAC (global), to share information on security threats. Importantly, awareness campaigns for employees are organised as detrimental activities may begin with an email arriving in a bank employee's inbox with a malicious code.

Moreover, it is important to stress that several legislative initiatives have already been adopted to mitigate risks (Security of Network and Information Systems Directive (NIS), GDPR). No further regulation is needed therefore but cross-sector practical guidance would be welcome to help financial institutions to interpret the existing requirements, in particular, considering that those legislations are still in the implementing phase.

It is also important to keep in mind that cybersecurity is no respecter of borders. Rather, it is a global issue relevant to governmental, public and private sectors, in the same way that digital services interconnect various countries. As a result, collaboration, cooperation and convergence within and between the European and International levels are required. Cooperative actions among the interested stakeholders and bodies is essential in order to guarantee the highest level of customer and bank security. Efficient frameworks and networks for information sharing and reporting (threats, incidents, lessons learned, and countermeasures, avoiding unnecessary reporting burdens and overlap) are what is required. It is indeed essential to ensure that any conflicts with the General Data Protection Regulation (GDPR) do not raise obstacles to the unfolding of an effective cybersecurity or hinder the exchange of relevant security-related information.

It would be relevant to:

- streamline harmonised format and procedures for security (IT) incident reporting to avoid overlap and redundancy in reporting to multiple competent authorities (Security of Network and Information Systems Directive (NIS), PSD2, Data protection regulation, Single Supervisory Mechanism – Single Supervisory Mechanism (SSM)).
- share definition and criteria to determine the major incident to be reported (this would allow comparability of data, evaluation of scenarios and drawing from the lessons learned);

- set common and homogeneous criteria to understand the level of significance and severity of a security incident;
- harmonise the different formats and procedures for incident notification, in order to avoid redundancies; in this regard, the aggregation of incident notification in a single point of contact would be very much supported;
- establish a constant dialogue between the European Central Bank in the context of the Single Supervisory Mechanism (ECB/SSM) and the relevant stakeholders (banks, banking associations, European Banking Federation, etc.) on methodologies/processes for incident reporting and cyber risk assessment;
- establish a worthy mechanism able to extract and distribute to banks, lessons learned, deriving from incident reporting, in order to support incident and fraud prevention and early warning.

The banking industry for its resilience purpose and risk mitigation needs a legal framework which allows the possibility to share among themselves and/or public authorities where appropriate sensitive information related to fraud & cyber-attacks at national and cross-border level. For this purpose, the banking industry would call upon an active dialogue between the industry, the Article 29 Working Party (Future European Data Protection Board), European Banking Authority (EBA) and the European Central Bank in the context of the Single Supervision Mechanism (SSM) with a view to assessing how best to enable this sharing of relevant (including possibly sensitive) information, possibly drawing on the experience from the newly established private initiative of the UK Cyber Defence Alliance.

The only additional concern we see is that as this kind of technology allows to put together massive amount of data from different sources, special care must therefore be undertaken when reviewing the access control and security mechanisms in the Data Lake as it would targeted by attackers as it might store huge amount of customers information.

14. Would you see merit in prohibiting the use of Big Data for certain types of financial products and or services, or certain types of customers, or in any other circumstances?

We do not see any benefit in prohibiting the use of Big Data for certain services or financial products, as these are often used in order to protect consumers (for example, under MiFID rules, investment firms have to require and collect a great amount of Data in order to assess the best financial products to be offered to their clients); moreover, the increase of new regulatory requirements seems to encourage the use of more data and information.

15. Do you agree that Big Data may reduce the capacity of consumers to compare between financial products/services? Please explain your response.

In general personalised offering are still more beneficial to consumers than generic ones as they enhance the added value and consumer offering experience.

We also think that customers would take better decisions if they can rely on an amount of well-explained data.

In addition, as expressed in our response to question 9, it is important to note that tools such as comparison websites or account aggregators, based on Big Data techniques are being developed, to facilitate comparability.

16. How do you believe that Big Data could impact the provision of advice to consumers of financial products? Please explain your response.

The combination of various customer datasets could improve the understanding of customer's needs, the quality of products and services and facilitate the development of personalised offers in real time. Big Data analytics also offer opportunities to identify potential warning signs in terms of fraud or credit-worthiness assessment.

Thus, Big Data can create personalised and more targeted offers for customers and avoid over-marketing of unwanted products and will increase the ability to provide personalised advice based on how consumers actually behave (rather than how they say they behave).

In line with our response to question 9, while consumers making unsuitable decisions potentially represents a risk for any kind of services provided online, it should be considered that this is mitigated by the possibility for the customers to have a permanent access to an operator (via an online chat, mail or telephone) who would provide assistance throughout the process. In some cases, providing automated financial advice might even avoid any potential conflicts of interest due to human intervention. It is also important to stress that, in general, as for any financial advice, specific legal requirements would have to be fulfilled.

However, regarding online platforms and websites some of our main concerns remain, such as:

- the risk for clients to consider and treat as advice other type of services: The risk of confusion could arise from the fact that the customer based his/her decision on price comparison with limited information or wrongly perceive an information given by the firm as personal advice.
- receiving advice without realising it is an advice: the client should provide a clear consent and express his understanding before receiving the advice; the risk would be mitigated if the specific service being provided is clearly explained to the client. It is also important to emphasize that the GDPR has very clear rules on the use of personal data in the context of automated decision making. These rules adequately mitigate the risks. Banks want to treat their customers fairly too. The principle of due care also plays an important role as a mitigating agent.

17. How do you believe Big Data tools will impact the implementation of product governance requirements? Please explain your response.

We believe that Big Data tools will impact the implementation of product governance requirements significantly. Big Data tools will help entities to define more precisely their product assortment (products that will be offered, to whom and through the provision of which investment service) taking into consideration the information gathered about needs, characteristics and objectives of consumer subgroups. It will enable manufacturers and distributors to improve the product monitoring assessing whether the product remains consistent with the needs, characteristics and objectives of the identified target market (analysis of information about consumer satisfaction and if the product has been distributed to the defined target market).

Big Data will be necessary to ensure the quality and accuracy of the data and the reliability of the algorithms. These two elements can only be achieved through proper organizational measures and processes.

It is however important to keep in mind that impacts on products governance are not exclusive to Big Data and its use, like any other process or operation, is subject to conduct of business principles. Specifically, Big Data will enable banks to demonstrate clearly that products have been developed for specific customer segments based on customer needs.

18. How do you believe Big Data tools will impact know-your-customer processes? Please explain your response.

We believe that with the use of Big Data tools, current Know-Your-Customer processes may benefit by providing a more complete and accurate view of the customer, in both customer's on boarding process and the follow-up of the business relationship or to improve the Risk Based Approach (RBA) for customer management. It helps consolidating available customers' data from all enterprise sources and move away from the conventional use of a standard transactional profile for bank's customers towards the creation of holistic digital profiles.

Analytics are changing the way financial institutions interact with their customers. The multichannel interaction and the historical data are converging giving banks a multidimensional vision of their customers.

19. What are key success factors for a Big Data strategy (i.e. the adaptation of the business model/plan towards Big data driven technologies and methods)?

We consider that key success factors for a Big Data strategy are:

- the identification of key business challenges involved, the sequence in which those challenges will be addressed, and the business process requirements that define how big data will be used;
- the incorporation of Big Data tools into the core of banks business strategy which aims to provide a better customer experience, ongoing innovation for better customer outcomes and a greater understanding of its business;
- the transformation of their capabilities to exploit Big Data (more efficient internal processes; the full and timely integration of the database; the creation of a data-driven decision processes); techniques against overfitting of the parameters. Typically data-driven processes generate models too tightly linked to the database;
- the implementation of an effective Data Governance framework (high-quality data (with certification processes, maintenance, etc.) and pervasiveness (significant coverage));
- the recognition of the value that the activity provides to banks, fair impact measurement: key to internally prove value of big data without under nor overselling its added value;
- the definition of criteria for evaluating return on investments;
- the alignment of the needs of business users with the implementation roadmap of IT, safety of the data, intelligence of processing via algorithms;
- the engagement of business executives early in the development process. An effective big data strategy should be a highly dynamic roadmap for the future and a work in progress to be adapted. Business adoption of big data requires addressing issues of organisational alignment, business process design, coordination and communication;

- the development of specialized skills is also required; a clear vision to set objectives and target developments (partnership, data collection, etc.);
- A continuing dialogue with the customers about the advantages for them with the bank's use of Big Data.

20. What are the greatest future challenges in the development and implementation of Big Data strategies?

The challenge is to improve our analysis processes and our predictive capabilities keeping the focus on a managed data growth and governance.

Big Data must be well-modeled, documented and maintained in order to be correctly analysed. It is crucial to extend a data governance to any data as well as link data quality and compliancy to data governance.

Big Data must be contextualised and semantically connected to other Data. Any source must be classified and any data must be governed according business and/or regulatory frameworks.

The challenges in the development and implementation of Big Data strategies are notably the following:

(a) Technical challenges

- integration with existing legacy systems;
- compromise of quality due to volume and variety of data;
- flexibility of infrastructure to interact with extreme volume/variety of data formats;
- evaluate cloud computing capabilities;
- many new technology market players do not have mature enterprise-ready capabilities around implementation, support, training, etc.

(b) Business challenges

- the Big Data business case is difficult to determine at first;
- Big Data adoption requires a cultural change: firms need a cultural change in terms of the innovative mindset, new business roles and advanced skills required throughout the organization—including senior management—to capture and understand the real business value behind the adoption of Big Data; firms may need to set up new business roles with the responsibility for defining and executing data strategy, identifying and managing data and designing data quality controls, and managing the traceability and reliability of business data; accountability for data ownership and management also needs to be established. Senior management with critical judgement on the overlap: technology, science and risk management (not only valuation of the risks but, more relevant their hedging);
- find the right use cases which are most suitable to the organization;
- identify relevant data protection requirements and develop an appropriate governance strategy;
- identify privacy issues related to direct and indirect use of big data sources;
- avoid internal overbuying of the big data approaches: as the whole industry and regulation sharply move towards big data strategies, the management of the different

units that first avoided digitization could rapidly change attitude and embrace inorganic change. Big data managers need to control this change to avoid deceptions. Big data is a tool, not a solution itself.

(c) Other challenges

- organizations may struggle with finding the right skills and building internal capabilities for handling big data as most of the technologies and methods are relatively new, and market resources are in short supply. Such skills are advanced statistical skills, distributed processing programmer skills, information architecture and management expertise;
- the costs associated with managing and monitoring the quality, credibility and integrity of big data can be prohibitive;
- increasing global regulations raise the stakes around security as the cost of dealing with data breaches continues to grow;
- diverse sources of data results in distributed storage and management, compounding security vulnerabilities;
- competitive landscape with new entrants in the field of financial services that have business models purely based on Big Data and choose to perform activities at the edge of the regulatory perimeter or with the minimum legal requirements; banks will have to react to this having in mind that the reputational risk they incur is higher than for other kind of players, as a reputational problem related to a failure in the big data management by a bank could contaminate the rest of the relationship with the customer; customers have traditionally been very shy on sharing their financial status; they perceive these data to require higher level of protection than social data however, as data portability will allow the data to flow from one player to the other, it will be very important that the customer is clearly aware of who is using his/her financial data;
- Restrictive interpretation of the GDPR by (privacy) regulators may block being able to use big data adequately;
- Negative public opinion on the use of data in the banking sector and not daring to test in sandboxes for fear of restrictive interpretations of rules and regulations.

21. This Discussion paper refers to a number of measures and tools meant to ensure compliance with conduct and organisational regulatory requirements as well as data and consumer protection rules in the context of big data analytics. Are other measures and tools needed? If so, what are they and what they should cover?

Please see our response to question 7.

The regulator is already forcing financial institutions to rely on Big Data techniques. An example is record keeping obligations: institutions need to be able to rebuild the history of a transaction for fraud prevention or AML purposes.

In addition, we think that there will be other opportunities for further metrics and tools especially applied to new technology use: firstly, Artificial Intelligence (AI)and then Blockchain

Another suggestion is to enable a balanced programme of consumer education in relation to Big Data.

Indeed, the discussion paper also highlights issues around reputational risks. In our view there is a communication and consumer education component to these. Much of the public historic discourse on the use of Big Data has disproportionately focused on hypothetical harms that distract from the real issues and could discourage firms from developing beneficial tools. For example, there are stories in the media about the risks and dangers of Big Data, which do not necessarily provide a balanced view of the benefits to consumers and society that Big Data can provide. Although there is no need to explain the workings of specific Big Data analyses in detail, for the potential benefits of Big Data to be fully realised it will be important to reassure consumers that these technologies can be beneficial rather than threatening, where they are well designed and subject to proper governance. Big Data's role beyond product development should also be communicated, particularly in the prevention of fraud and money laundering.

22. How do you see the development of artificial intelligence or blockchain technology in connection with Big Data processes?

- Artificial Intelligence (AI) technologies such as natural language processing, speech recognition, machine learning and cognitive computing, parse through massive quantities of unstructured data on which analysts depend. Using data from multiple sources, AI technologies can build a store of knowledge that may ultimately enable accurate predictions about consumers that are based not just on what they buy, but on how much time they spend in a particular part of a site or store, what they look at while they are there, what they do buy compared with what they do not - and other bits of data that Artificial Intelligence technologies can synthesize such as the Internet of Things (machines themselves produce data which may be connected to the behaviour and/or data of individuals).

  We think that they are rapidly becoming one of the most useful advances in building predictive analytic models and helping data scientists to be more efficient by automating some of the more manual tasks.

  AI within big data is simply a natural step. They will keep evolving hand-in-hand. When it comes to big data and AI, we are at the early stages, at the emergence of what the potential value of convergence can be.

  As AI progresses and evolves, some of the basic tasks that data scientists perform routinely, might be automated and will yield productivity (automating the more basic tasks and reserving the more complex ones for data scientists).

- As far as the Blockchain technology is concerned, it has the potential to revolutionize the financial sector by redefining companies and economies. However, shifting to a decentralised network will require educating end-users and operators, as well as integrating into current working process to have the biggest and best impact.

- On the surface there appears to be a lot of synergies between Distributed Ledger Technology (DLT) and Big Data particularly since one of the promises of DLT is that it stores a complete record of all transactions that have ever occurred on the system. While this may be true for the public ledgers (e.g. Bitcoin) it will not be true for private, permissioned ledgers that will be run by banks. In these cases, customer and transaction data will be obfuscated and encrypted and only visible between counterparts to a transaction.
  Except, that is, in the case where transaction data is willingly shared by the counterparts with the regulators. In which case, a regulator might be able/willing to run Big Data operations in order to look for patterns of unusual behaviour or fraud.

In our views, both Artificial Intelligence and Blockchain are key elements, but their current level of development (especially for AI) and application (Blockchain) are not mature enough.

23. Are there any other comments you would like to convey on the topic of use of Big Data by financial institutions? In particular, are there other relevant issues that are not covered by this Discussion Paper?

In our views, regulators should see Big Data as a major opportunity for the role of all players in the financial services sector, including regulators and supervisors themselves.

As a potential solution to assess the impact of data analytics, we believe the supervisors can help the data-driven innovations to be deployed across the financial sector by creating a framework of experimentation/regulatory sandboxes as safe spaces where regulated and non-regulated actors can test innovations in a controlled environment. This will also help supervisors to have access to innovative initiatives and assess them after seeing how they work (with certain consideration for strong protection of consumers/data subjects).

In addition, European Supervisory Authorities can play an invaluable role by providing support to national authorities to share experiences and resources and thus making innovation accessible to all countries. This is critical in order to set up a true European space for financial services.

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