DEUTSCHE BÖRSE GROUP

Gruppe Deutsche Börse

Comments on European Commission´s consultation towards „A new digital finance strategy for Europe/FinTech action plan“

Frankfurt am Main, 26 June 2020

General remarks

Deutsche Börse Group (DBG) appreciates the opportunity to respond to the consultation „A new digital finance strategy for Europe/FinTech action plan“ by the European Commission.

DBG in its capacity as a financial market infrastructure (FMI) provider uses modern IT and technological solutions to operate, and service the financial sector worldwide.

DBG's technologies are at the core of its operations, where they are used to organize the regulated markets, are an integral part of the regulated services we operate. We ensure trust in markets and the efficient functioning of these markets; including but not limited to market data, stock exchange indices, clearing, securities custody, etc.

Regarding new technologies, we are currently working on the use of cloud technology, AI and distributed ledger technology (DLT)/blockchain as well as automation of processes, which are all data driven. We use these technologies in a rather gradual, granular and tested manner, hence continuing to guarantee transparency, stability and investor protection at all times.

Please find hereunder our DBG key messages with regard to the digital finance strategy.

In case you have any questions, do not hesitate to reach out to us.

.

Key Messages on the Digital Finance Strategy/FinTech action plan

I. Overarching remarks

Build on existing regulation: we are in favor to build upon already existing rules and regulations (e.g. GDPR, competition law etc.) as well as sector specific frameworks (e.g. MiFID II/MiFIR, SFTR, trade secrets directive) to which market participants are already familiar.

Bespoke regimes create uncertainties: as they need time to be created, understood and applied. Also, the legislative process might create contradictions to existing legislations. Clear and consistent rules, based on existing regulatory frameworks, are most innovation friendly.

Tech-neutrality: this is very important, as regulation should be independent of the used technology. However, not all challenges can be tackled by ensuring the principle of tech-neutrality, but have to be addressed technology specific, as every technology presents its own challenges.

"New risks": only "new" risks resulting from the technology need to be mitigated by adjustments into existing regulations.

"Same business, same risk, same rules" for technology companies: technology companies/FinTech companies should also be subject to the established financial regulatory requirements, when offering similar services ("same business, same risk, same rules").

Major obstacles for innovative technologies: fragmentation among Member States (e.g. different implementation/"gold plating"), legal uncertainty, asymmetry between cloud service providers and their customer.

Sandboxes: sandboxes are a solution in the technical testing phase, however if the service is offered to customers in "reality"/goes live, existing rules have to be applied to prevent a legal free-ride problem (e.g. GDPR).

Dialogue between companies and regulators: the constant dialogue between companies/business associations and regulators/competent authorities is beneficial. Companies should explain their concrete use-cases to authorities, in order not only to make them aware about new trends, but also to support the evolvement of the regulatory framework.

Vertical and horizontal cooperation of authorities: not only the cooperation between market participants and authorities at different levels is important, but also the alignment and cooperation of authorities in different jurisdictions and at different levels as well as sectors is beneficial.

Extend passporting regime to new digital services: it would be beneficial to extend the existing EU licenses passporting rights to new digital services (e.g. the crypto custodian business).

Different digital identities: we would like to highlight the need for a reliable identifier in a digital EU economy, based on clear common rules. It would not be very efficient to create multiple digital identities for consumers/businesses.

Mandatory identifiers: a further increased mandatory use of identifiers over time (e.g. LEI), especially of those building the new identity, is relevant, as it allows for more standardized processes and efficiency gains. If the use of identifiers would be made mandatory in the future, the rules should clearly state that the companies are obliged to have such an identifier.

(Digital) Financial literacy: we think that (digital) financial literacy should be anchored in school lessons to a sufficient extent and on a compulsory basis for all pupils in Europe. There is a growing connection between financial literacy and digital competencies, both are needed for a better understanding of the "new digital" financial services.

Digital transformation can support European Green Deal: we very much welcome the EC's approach to explore measures needed to ensure that the digital transformation is environmentally sustainable. We are convinced that combining the new digital finance strategy with specific actions to mobilize and accelerate flows of private finance into sustainable investments may contribute mutually re-enforcing of both strategic objectives.

Technology firms can complement financial industry: while disruption and "creative destruction" are often associated with technology companies entering established markets, there are also concrete examples of collaboration that benefit the existing ecosystem. In these cases, we would refer to technical "evolution" instead of disruption. One such example is Deutsche Börse's strategic partnership with HQLA^{X}, a financial technology firm founded in 2017.

II. Crypto-assets

Regulation: we prefer a binding EU-regulatory framework for digital assets, as opposed to "soft law". As we advocate for EU regulatory harmonization which will embraces innovation and speeds the time needed for businesses to go to market. Targeted legislative changes are the most efficient and practicable solution, providing legal certainty, while guidance or interpretative communications are helpful provided no legislative framework is in place.

EU digital-assets classification: our overarching proposal is that digital-assets represent the digitalised embodiment of an asset. Crypto-assets (like coin & token) are a subcategory of digital-assets, based on cryptography.

Financial instruments: if "digital/crypto-assets" represent a currently existing financial instruments (e.g. shares, commodities etc.), then these "digital assets/crypto-assets" should adhere to the existing framework of MiFID II/EMIR/CSDR etc.

Non-financial crypto-assets: a fully harmonised EU law is needed, to make the new asset class trustworthy.

"Digital money": our proposal of "digital payment assets" includes crypto-currencies, (global) stablecoins and central bank digital currencies (CBDC), differentiating "digital money" on features, like "type of asset": native/backed with real asset(s); "who is the issuer": central banks/financial institutions/non-financial institutions; "reach": global/regional/wholesale/internal.

Stablecoins: use the existing and potentially modernized EMD2 framework as it would allow for a consistent framework for all kinds of "digital money", therefore a bespoke regime is not needed.

"Hybrids": should a hybrid-digital-asset contains elements of a financial instrument (at any given point of its live-cycle), it should fall under the rules for the respective financial instrument.

"New Service Providers": all "new service providers", like "custodial wallet providers" and "trusted third parties" should adhere the existing regulatory framework and obtain any required license, should they offer financial/regulated business, as trading venues, CCPs, CSDs.

Digital-/Crypto-assets within FMIs: FMIs should also explicitly be allowed to "handle" digital-/crypto-assets in future (e.g. CCPs to accept crypto-assets as margins or CSDs to offer services on "crypto-assets").

III. Cloud

Cloud market: The cloud market offers technological solutions in financial markets to innovate and should be supported.

Harmonized rules for cloud outsourcing: there is the need for EU harmonized rules for outsourcing into the cloud. It must be mitigated that national measures on outsourcing hinder the usage of this technology and the respective services. This is not only relevant for the financial sector, but for the economy as a whole.

Levels of protection: while the level of protection is already high, further advancements are required in the areas of: a) Extending encryption technologies to data being in use/in memory b) Add end-to-end encryption where possible c) Consistently implementing customer lock-box/consent requirements before data is accessed d) Agreements between EU and other jurisdictions (e.g. US) needed to strongly regulate cross border access and activities.

Problems/risks of the current cloud market: asymmetry of power of negotiation between customer and CSPs, i.e. high efforts and time are required to agree regulatory compliant contracts with CSPs in the financial sector. Therefore, we actively support the EU´s work designing "Voluntary Standard Contract Clauses" to facilitate future negotiations. Also, it is very difficult to procure/adopt new and innovative cloud solutions, as it takes a long time to ensure that these new services are regulatory compliant. Often, new solutions are not meeting regulatory expectations right from the start.

Clear guidance on existing rules: clear guidance for companies based on existing rules would be beneficial. Further, there is a clear need for EU rules covering cloud outsourcing, which on the one hand promote the uptake of the technology to make the financial industry more competitive and on the other hand incorporates existing standards (like the German BSI C5 standard), which are already used by the industry.

IV. Artificial intelligence

Mutual understanding: The cooperation between authorities and market participants can bring valuable outcomes as they may lay the ground for a wider ecosystem. These ecosystems should be promoted and supported. Together with the Hessian Ministries, DBG and other have such a cooperation within the so called "Financial Big Data Cluster".

Apply existing rules: From our point of view as a financial market infrastructure, most activities/services performed by AI applications in the financial sector would be regulated by already existing rules and legislation, therefore it might be useful to ask whether a completely "new", and therefore unregulated, task is performed by an AI application in contrast to an already "known", and therefore regulated task. In the latter case, adjustments to the existing framework might be sufficient.

Review of requirements: any list of requirements for (high-risk) AI applications should be reviewed and updated timely and frequently, e.g. without a level 1 change of the regulatory framework, to keep up with technological innovation.

Efficiency of assessment-processes: it is crucial that the necessary capacities are in place to assess AI, to ensure efficiency in order to support the launch of AI products.

We support a certification of high-risk AI applications: further, for non-high risk AI applications it should be allowed for companies to receive a voluntary certification. We prefer an official harmonized labelling system for both applications with clear requirements and an official certification process performed by a formally authorized actor. This service could be offered by a public authority directly or by a private institution with a public permission on behalf of public authorities (like the German TÜV).

Self-certification: we are opposing "self-certification" systems, as they lead to a lot of certificates and blurring the information for users (negative developments in the area of "bio"). If a "self-certification" system is used, there should be an external validation by auditors.

AI review live-cycle: every AI provider needs to think about internal processes (models, training of data, handling of critical situations, handbooks, documentation etc.), the official certification, both ex-ante and ex-post assessments, later more ex-post than ex-ante assessments, after 5 years revision of processes, if necessary.

Risk Assessment: any AI application must have clear and well-designed rules/objectives to minimize the associated risks. High-risk AI applications: A combination of ex-ante assessments, based on an external conformity procedure, as well as ex-post market surveillance would be useful. Non high-risk AI applications: A combination of ex-ante assessments, based on a self-assessment, as well as ex-post market surveillance would be useful. In cases where ex-ante assessments are difficult, more ex-post assessments are needed. Either way, it is crucial that the necessary capacities are in place to assess the AI, to ensure the efficiency to support the launch of AI products.

Open/closed systems: It is important to differentiate between AI applications operating in "open systems" (e.g. road traffic) or "closed systems" (e.g. playing chess). In "open systems", the AI will never be able to cover all eventualities, as the training data is always limited. Here humans must make the final decision. This is also true for high-risk AI applications in "closed systems".

V. Operational resilience

Proportionality needed: proportionality should be an important principle during the design of operational resilience requirements.

Interaction between horizontal and vertical frameworks: it would be helpful, if the future interaction of horizontal operational resilience frameworks with national and/or sectoral frameworks would be streamlined.

IT auditing standards: IT auditing standards are needed, should be clearly defined and cover key elements, to allow for mutual recognition of audits among authorities. This would also allow for a "re-use" of one single auditing report provided by companies for different authorities.

Reporting and sharing: if companies report IT incidents to one competent authority, this authority should share the results/analysis/best practices amongst (ideally) all market participants, but at least to those who reported.

VI. Data

EU Data Strategy: we support the idea that the European Union needs an overarching data strategy in order to achieve the benefits of the single market and avoid fragmentation.

Harmonized approach: we are strongly in favor of a harmonized approach in order to speed up the processes with the use of innovative technologies and not lagging behind with regard to innovation/applying new technologies globally.

Data classification: we see the need for developing a clear definition/glossary of "data" which could foster a common understanding in the industry and lead to efficiency gains. In our view,

it is important to develop a classification of data which on a high/meta level could identify necessary information on its origin, sector, timely availability, etc.

No "one-size fits all" approach: as the nature of data is extremely diverse and complex, we do not think that a "one-size fits all strategy" is possible or suitable. Given the differences across industries, sectors and consumers, targeted measures within some areas are more likely to be successful at the beginning.

Commercial use of data: business which produces and commercializes data must still be possible within the EU, to provide incentives for companies to stay innovative and develop new data related services. While we support the idea to make data more available, other issues have to be taken into consideration as well: sustainability, innovation, trade secrets, risk prevention, fair competition, data quality and sufficient incentivization to invest into data quality, responsibility and liability. Especially, as EU companies are competing on a global scale.

Data should be generally available for new businesses: data enables companies to refine their business models, to improve and individualize their offers or to develop completely new business models. Therefore, data should be made available to interested parties, business models and application scenarios. Especially certain types of start-ups depend on the availability of data. There may be options to explore of a differentiated data license model with a special focus on SMEs/start-ups. At the same time data protection laws have to secure to privacy and informational self-determination of citizens (sovereignty of personal data), are important as well as trade secrets protection.

Investments in innovations necessary: Companies will only invest in the collection and analysis of data if they expect this investment to have an economic or competitive advantage. If such an advantage cannot be achieved or is at risk because e.g. produced data must be shared with competitors, the companies will stop or limit the investment or the production of the data (free-rider problem). No company would invest in the production of data if it then simply had to make the results of these efforts available to the competition free of charge.

Therefore, companies should be allowed to "upgrade" raw data and develop products/services on these data and ask for fees/charges, in full recognition of the existing property/contractual rights and obligations. Otherwise, this would send negative incentives towards data collection/standardization and product developments: i.e. "commercialization of data" should be allowed. To facilitate data sharing amongst companies, we see the need for a new enabling environment supported by data infrastructures. A possible example in this regard might be the "Financial Big Data Cluster" (FBDC) initiative, see below.

Copyrights: through digitization new ways of access to and onward distribution of valuable content/data with copy- or other rights have evolved often to the detriment of the originator. While there is value in innovation, we deem it very important that necessary rights to generated information is being protected under the EU Digital Agenda and the Data Strategy of the EU.

Balance between data accessibility and contractual rights of companies: We are of the opinion that an unconditional claim to data access or a corresponding obligation to grant data access must be rejected. The principle of freedom of contract ensures sufficient access to data. Through this factual assignment of data to the data producer, the data producer has the necessary control right over the data, which he can control by means of contract law. Data can be made available to any interested party under a license agreement which ensures companies that invested in the production and/or collection of data not to expect economic disadvantage. This approach ensures a proportionate balance between making data accessible to the public while ensuring the rights of the companies that invested in the production of data.

Compensation for data providers: as recommended by the EU Commission, the contribution of data to the public should be promoted, but the application of license fees or any other compensations should be allowed further. Especially, when the data source is depending on the income for data. The fees should be reasonable and shall be proportionate to the value which the data represents to the purchaser/user. The value of data depends primarily on its usefulness for a business model or on the possibility of gaining usable and affordable information from it.

Difficulties in the use of data: difficulties with regard of the use of data due to restrictive EU regulations e.g. banking secrecy versus developing big data solutions to fight anti-money-laundering. We see the need for clarification to comply with existing rules and simultaneously to develop further solutions, e.g. via criteria for the use of anonymized or pseudonymized data in order to facilitate broader analysis. AI needs per se more data and should be allowed to use data on an aggregated level. It is important to find a careful balance between "data privacy" and use of data for public interests.

Integrated access to non-financial data needed: digitalisation is the key to enabling a broad and efficient use of non-financial data. Potential users of non-financial data would not be able to gather such data from classic, non-digital sources like annual reports – at least not in an efficient and reliable way. Having to gather non-financial data from such classic sources would be extremely onerous so that individual entities would be prohibited economically from accessing the data. In this situation, a multitude of service providers would try to tackle the onerous task of collecting the non- financial data and would then make available the data – centrally accessible and in a machine-readable format.

Sector specific EU data space: we see the political interest, however one "single common EU data space" would not lead to innovation; a competitive approach would be preferable. One harmonized approach across different industry sectors might be too complex as well. We would prefer to start with "meaningful content clusters" within sectors and develop standards for those data, as this leaves sufficient flexibility to evolve.

Standardisation: we would prefer standard setting by industry bodies who know the details and work on common standards on a voluntary basis. Standards vary across industries in line with the different data/needs within each sector.

Data as a "common good": in order to allow analyses for the better of societies to monitor public developments, data might be common goods, however: to stay innovative, not all data could be defined as "common good" here a clear classification is needed to differentiate categories of data. In this context we deem it important for regulators to keep in mind as well the rights of individuals, being it as regards personal data, but as well those of taxpayers or other parties, when it comes to the funding of a common good. It is important as well that the concept of common good is not overly expanded and misused by companies promoting it, for their own business interests, while the bill is being paid by the taxpayer or any other third party. To stay innovative, not all data could be defined as "common good" here a clear classification is needed to differentiate categories of data.

Data protection: GDPR is a very good example that an EU-unified rule-set with high standards increases legal certainty, even if the common understanding/interpretation/application on national/regional level could still be further aligned during time. These EU "data protection" rules are signaling customers around the world that high standards are applied within the EU.

High-value data sets: Clear definition of scope necessary will be necessary, rights and duties of the data sources need to be considered. This includes the rights and liabilities of those re-using the data. It must be clear who is responsible within the user chain in case of damages caused.