DEUTSCHE BÖRSE GROUP

Deutsche Börse Group

Position paper on the European Commission´s legislatives proposals on DORA

12 February 2021

A. General remarks

Deutsche Börse Group (DBG) appreciates the European Commission´s ongoing efforts to make Europe fit for the digital age and develop a Digital Single Market. Therefore, we welcome the regulatory initiatives in the Digital Finance Package including those proposals which are of most importance for DBG and to which we have partly already responded in the respective "have your say" procedure:

- the pilot regime for DLT market infrastructures;
- Regulation Markets in Crypto-Assets (MiCA);
- Digital Operational Resilience Act for the financial services industry (DORA) and the
- Directive amending directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341.

It is important that technological progress and the opportunities it creates - such as efficiency gains, innovation and flexibility - do not unfold unregulated bringing potentially significant risks to financial stability and consumer protection. Rules and appropriate requirements for IT security are needed that promote confidence in the new technology and ensure supervisory powers to take corrective action in the event of misconduct and clearly assign responsibility. Considering the implications of the Digital Finance Package on stability and integrity of financial markets, we strive to remain at the forefront of the digital regulatory debate.

We see the current developments as an opportunity to ensure that existing and future markets continue to be organized in a resilient, secure and transparent manner - with increased flexibility and efficiency. Therefore, we appreciate that DORA is designed as "lex specialis", which ideally reduces uncertainty and double regulation. We think it is of utmost importance to find the right balance between "security" and the use of innovative technologies within the financial sector.

New digital technologies are a decisive factor here, but it has to be made sure that the all the lessons drawn from the financial crisis 2008 regarding financial stability and market integrity are still in place. Experience from past financial crises in particular has shown that fundamental principles such as consumer protection, financial stability or the conduct of an orderly monetary policy must under no circumstances be compromised and must be ensured in the interests of society, irrespective of the technology used. These principles should not be invalidated by the mere reference to the promises of new technologies.

Please find our key positions towards DORA hereunder and note that these are preliminary and will be more detailed in due course of the legislative processes. We have based our assessment on the latest documents made available by the European Commission on 24 September 2020.

B. Key Positions

- **Harmonized rules within the EU are needed** to make the Digital Single Market more secure
- DORA will be the "**lex specialis**" used by FMIs and puts a spotlight on ICT security
- DORA should keep the **balance between security for the financial system and the innovative use of technology**
- **Industry should help define the "state of the art" of technology**
- **Harmonized rules for cloud outsourcing necessary** for the finance sector
- **Voluntary standard contract clauses are appreciated**
- We welcome that the **principle of proportionality** is addressed, but fear too prescriptive rules
- The **precedence of sector specific financial regulation against horizontal rules is welcomed**
- **Alignment with global standards** on key definitions, international cooperation and acknowledgment of industry initiatives could be beneficial
- **Some requirements seem at least partially unfeasible**
- **More clarification is needed for the effective assessment of sub-contracting chains**
- **Conditions on sub-outsourcing in third countries are disproportionate** and would hinder global operations
- The **designation of critical ICT third-party service providers seems not fully defined**
- We see **significant challenges with regard to critical ICT third party service providers**
- **ICT third-party providers should not be obliged to let financial entities take copies of high-risk evidence**, but make these available in a secure, non-proliferating way
- **Level 1 provisions should be flexible enough to accommodate the different types of service providers within the scope of the oversight framework** for critical third-party providers
- Financial supervisors must be aware of the **potential consequences of requesting specific patches** from Cloud Service Providers (CSPs)
- **Streamline ICT-related incident reporting and address overlapping reporting requirements and harmonization of testing**
- Specific exit plans and timelines should be considered per service
- **Threat-led penetration tests should explicitly be allowed to also be performed by the financial entity itself**
- IT Asset Management procedures seem appropriate
- **Proportionality and risk-based approach necessary** to define penalties and measures on breaches

C. DBG views on DORA

Harmonized rules within the EU are needed to make the Digital Single Market more secure: As a general remark, we appreciate that the European Commission mostly relies on proposals for regulations in its Digital Finance Package, instead of directives. Fragmentation among Member States (e.g. different implementation/ "gold-plating") creates legal uncertainty, asymmetry and hinders economies of scale.

Further, we acknowledge that the European Commission builds upon already existing rules and regulations, as well as sector specific frameworks (e.g. MiFID II, NIS Directive, EMD, PSD2, AIFMD, UCITS and CRD) with which market participants are already familiar.

DORA will be the "lex specialis" used by FMIs and puts a spotlight on ICT security: The proposal for the regulation provides high standards, clarity and aligns supervision. However, it has to be ensured that the goals of innovation friendliness and security are achieved and not conflicting with each other. This is also true with regard to the upcoming rules on NIS 2.0 or the directive on the resilience of critical entities (RCE).

DORA should keep the balance between security for the financial system and the innovative use of technology: The provisions foreseen in DORA should not unintentionally make the use of an innovative technology in the EU´s financial sector unattractive or impossible. If some provisions would make it impossible for third-country service providers to offer their solutions effectively in the EU, this could lead to detriments for the financial industry (e.g. related to costs, less-attractive offerings for EU financial clients), compared to other jurisdictions.

Industry should help define the "state of the art" of technology: Due to the rapid technological changes, we recommend a risk-based approach by the companies to fulfil their security obligations and to help define "state of the art" technology, instead of regulators alone. Companies might otherwise struggle to comply with such rules and regulators might find themselves under time pressure to adjust existing requirements in on short notice.

Harmonized rules for cloud outsourcing necessary for the finance sector: We appreciate that DORA foresees dedicated rules for "critical ICT third-party service provider" including cloud service providers, which will lead to a more harmonized approach (see Art. 28ff.). This is an important step to mitigate fragmentation on outsourcing, hindering 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. However, further clarification and ideally alignment is needed to answer the question how DORA would relate to outsourcing guidelines already published by ESAs and other authorities.

Voluntary standard contract clauses are appreciated: We appreciate that the European Commission facilitates the use of voluntary standard contract clauses, as some elements of the contractual relationships between CSPs and firms can be standardized (see recital 55). This eases the adoption of cloud technology-based services.

However, it is still problematic to procure/adopt new and innovative cloud solutions as it takes a long time to ensure that these new services are regulatory compliant. Some provisions for CSPs might be too prescriptive and would inevitably lead to regulatory obstacles for these companies. Policymakers should carefully balance obligations, especially for third country CSPs.

Further, compliance to the General Data Protection Regulation (GDPR) by ICT-third party service providers or sub-contractors should be mentioned as a requirement in the Key Contractual provisions (Art.27).

We welcome that the principle of proportionality is addressed, but fear too prescriptive rules: The explanatory memorandum states: "*The proposed rules do not go beyond what is necessary in order to achieve the objectives of the proposal*". However, the respective qualitative and quantitative criteria have to be evaluated carefully, given that different companies are of different sizes and inherent risk exposures. A "one-size fits all" approach does not "fit" all and increases the burden for companies.

Therefore, we would be cautious towards overly prescriptive technological measures which would rapidly be outdated due to technological evolution. While there is a need for a coordinated approach on cyber-resilience, when considering further regulatory requirements in this space it is important that flexible innovation is safeguarded. Hence a risk-based and proportionate approach is needed.

Any requirement to disclose details on cyber resilience should be conducted carefully. A potential approach should be sufficiently broad to encompass multiple cyber risks, avoid recommending technology-specific parameters.

Nevertheless, compliance with some sectoral requirements can be challenging, as these are formulated in an excessively broad language. More detailed, but not technology-prescriptive, requirements would be helpful from an operational perspective and would foster supervisory convergence by creating a clear baseline framework. As a general remark, we would appreciate if DORA would be more precise in the security goals, entities have to achieve and less prescriptive in the ways how to achieve them.

The precedence of sector specific financial regulation against horizontal rules is welcomed: Compliance with the existing sectoral/horizontal legislation, such as the Network and Information Security (NIS) Directive, European Critical Infrastructure Directive, MiFID II/ MiFIR, CSDR or GDPR, has increased cyber resilience measures across the financial sector. However, the inclusion of digital operational resilience and/or cyber resilience in most recent legislative measures has led to a cumulation of requirements. Therefore, we appreciate that in the future the interaction of horizontal operational resilience frameworks with national and/or financial sector frameworks will be streamlined (see recital 16). We appreciate that DORA will be the reference point for IT security for the complete financial sector as a lex specialis.

To further support this effort, we would recommend consistency when streamlining all files. It is important to harmonise these legislations, inter alia the classification of incidents to avoid further duplication of efforts upon compliance and reporting.

Alignment with global standards on key definitions, international cooperation and acknowledgment of industry initiatives would be beneficial: As a general remark, we think that in some cases more precise and/or aligned wording would be beneficial to mitigate ambiguities to provide for more clarity. For example:

- Art. 8 (3) states that “state of the art” technology would “guarantee” the security of the means of transfer of information. It is questionable whether any technology could “guarantee” anything. We would rather speak of “enable”.
- Another problem would be the term “substantive changes” Art. 10 (5), which should be limited to “changes concerning Disaster Recovery mechanisms”.
- Also referring to Art. 10 (1), we think it would be better to clearly have a “Business Continuity Policy” for business and “ICT Continuity Policy” for ICT-related scope, instead of a “ICT Business Continuity Policy”.

- Also, we suggest aligning the terminology of regulation with the wording of international standards like provided from International Standards Organization (ISO) or BCM-specific "Good Practice Guidelines" provided from Business Continuity Institute (BCI). For example, the proposal foresees documented plans in a broad sense, but it would be beneficial to differentiate a "Business Continuity Plan" (planning for continuity of critical functions, an "ICT Continuity Plan" (planning for the recovery of ICT resources that provide services for critical functions and a "Cyber Response Plan" (planning on how to respond to Cyber Attacks.
- Furthermore, in Art. 11 (5) a) the wording on geographical distance is very vague.

Regulatory alignment with global standards could therefore be valuable in order to define key terms comprehensively and more precise.

In addition, we also encourage regulatory cooperation of EU authorities with international regulatory authorities on harmonising requirements and guidance on advanced testing frameworks, which would enable a smooth implementation for firms that operate different entities across borders and in different jurisdictions.

Further, several industry-led initiatives and solutions currently work through sharing experiences, cooperating, and collaborating with industry groups. For example, any proposed security risk management framework should be based on internationally developed standards (e.g. the National Institute of Standards and Technology Cybersecurity Framework (CSF)). Against this background, we would support an approach where certified measures are deemed to be sufficient. That way, a clear harmonised baseline would be defined, acknowledging "state of the art" internationally agreed solutions, thereby improving the overall level of resilience

Some requirements seem at least partially unfeasible, particularly:

- Art. 11 (3) on backup policies: backup system needs to be directly connected to the main system in order to (e.g.) replicate data. The wording "operating environment different from main one" is very vague and should be made more precise. It should be also made clear that a second geography/location from the same CSP is fulfilling this requirement.
- Art. 21 (4) on general requirements for the performance of digital operational resilience testing: the term "undertaken" is not realistic. These tests must be performed by the staff operating the systems. The wording should be changed into "overseen".

- Art. 25 (8) on general principles: the wording "ensure (…) are terminated" is too strict. Financial entities shall be required to evaluate, risk assess and to decide on cancellation, but not automatically have to cancel a contract when e.g. the ICT third-party provider breaches its contractual terms. We would therefore recommend providing more flexibility to the regulated financial entities instead of mandating the termination requirements, as well as harmonising such requirements with other existing rules and guidelines.

More clarification is needed for the effective assessment of sub-contracting chains: Art. 26 (2) mandates financial entities to assess whether and how complex chains of sub-contracting may impact their ability to fully monitor the contracted functions, and the ability of competent authorities to effectively supervise the financial entity in that respect. We would suggest providing more clarification on how this requirement should be put into practice, as it seems currently very burdensome operationally and whether this stands in comparison to the overarching goal.

Conditions on sub-outsourcing in third countries are disproportionate and would hinder global operations: Provisions foreseen in Art. 31 (1) (d) (iv) could effectively mean financial entities cannot outsource any critical functions to ICT providers, as long as they cannot ensure that there is no sub-outsourcing to third countries. This is not proportional and would effectively rule out use of CSPs for critical functions. Further, in today´s financial industry, the use of third-country service providers is a common practice within "global operations", it is unclear why CSPs should not be effectively allowed to use sub-outsourcers as well to serve their clients.

For example, some financial entities require a "follow the sun" customer support service for their cloud architecture, i.e. customer support service available on a 24 h/7 days basis. To operationalize this model, ICTs provider often need to rely on its operations from another location. However, the DORA provisions would mean that EU financial firms could no longer have this option, unlike their non-EU competitors.

The designation of critical ICT third-party service providers seems not fully defined: Art. 28 states that the ESAs, through the Joint Committee and upon recommendation from the Oversight Forum shall designate the ICT third-party service providers that are critical for financial entities, and such designation has to be based on a series of criteria, among which the "number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider".

However, we believe that such definition is not precise enough and would request the European Commission to provide clarifications.

For example, the service providers located in third countries ensuring the "follow the sun" service availability could themselves be considered ICT-third party providers based on the criteria in Art. 28 (2) c), as financial entities would rely on them directly or indirectly to maintain service stability. Making use of those providers would be prohibited pursuant to Art. 29 (9). According to Art. 29 (9) financial entities shall not make use of providers established in a third country, which will result in loss of resilience due to lack of "follow the sun" – 24/7 maintenance. This may be the case even if it was an affiliate company of the main contractor. In addition, the interdependence with Art. 31 (1) (d) (iv) is unclear.

Additionally, to clarifying the criteria of para. 2, it should be ensured that art. 28 para. 9 does not include affiliate companies, to which sub-outsourcing takes place. This is essential in order to maintain equality of competition regarding non-EU competitors.

We see significant challenges with regard to critical ICT third party service providers: The provisions proposed in Art. 28 (9), which would prevent financial entities from using third country ICT third party service providers in case those would be designated as critical, creates significant challenges for the following reasons:

Firstly, it is not possible for financial institutions to determine an ICT provider's status as critical for the financial sector as a whole. This assessment is undertaken by the ESA's Joint Committee, based on information that is not available to individual financial institutions.

Secondly, the provision lacks clarity on how to manage situations in which the designation of a provider as critical takes place in the context of existing contractual arrangements. It should therefore be clarified that the designation of a third-country providers as critical is undertaken by the ESAs and not the financial institutions.

Thirdly, and as stated above, there are not that many providers active that can fully service every cross-border financial service.

Therefore, it is essential that EU financial market participants are not prevented from using non-European providers. Forcing EU financial market participants to make use of EU providers will inhibit their ability to innovate, and to become more efficient. And this will be essential for financial market participants to maintain profitable as mentioned by the ECB, because "Merely adopting advanced technologies to improve internal processes is not enough. Satisfying the needs of sophisticated customers in today's increasingly competitive environment will require innovation to place the focus on the customer service experience."

ICT third-party providers should not be obliged to let financial entities take copies of high-risk evidence, but make these available in a secure, non-proliferating way: Referring to (Art. 27 (2) h-i), we think that for high-risk evidence, e.g. non remedied vulnerabilities, ICT third-party providers have a legitimate interest to avoid clients making copies. However, ICP third-party providers should be obliged to make them available e.g. by means of a secure reading room that customers can access whenever required. Additionally, if authorities would see the need to inspect sites of CSPs, this would reduce the burden for financial entities to visit the CSPs themselves.

Level 1 provisions should be flexible enough to accommodate the different types of service providers within the scope of the oversight framework for critical third-party providers: From our point of view, it would be beneficial, if the scope of the proposed oversight regime for critical third-party service providers, as proposed in the Level 1 provisions, would be adaptable enough to accommodate the different types of providers under scope.

Requirements that may seem appropriate for a certain type of provider, may not be suitable for others. For example, in the context of on-site inspections, the provision that would require providers to give hardcopies of records and procedures (Art. 34 (2) b), as well as the ability to seal premises (Art. 35 (2)) could not be suitable to a cloud environment. Further, the powers given under DORA would go beyond those present in the ECB's Supervisory Manual, acknowledging the need for judicial authorization in several Member States in the case of sealing of premises.

Financial supervisors must be aware of the potential consequences of requesting specific patches from CSPs: DORA gives the lead overseer some powers to make recommendations to an ICT provider on areas such as patch roll-outs, sub-outsourcing and physical security. Some of those areas are important to a CSP's ability to provide the highest security to its clients across all industry sectors – and a CSP would struggle to implement a security patch roll-out only for its clients in a specific sector. The risk of a financial supervisor asking for a specific patch roll for financial services clients in Europe is that those clients may face lower security standards than other non-EU clients

Measures taken by an EU financial supervisor under DORA power impacting the CSPs' functioning will need to take into account the fact that a CSP serves clients from various sectors and has contractual obligations to protect the security of all those clients' data – including to prevent major cyber threats.

Streamline ICT-related incident reporting and address overlapping reporting requirements and harmonization of testing: We welcome the intention that the European Commission wants to streamline and harmonize reporting duties mentioned in Art. 17-20: if companies report IT incidents to one competent authority, this authority should share the results/analysis/best practices with (ideally and where appropriate/necessary) supervisors and all market participants.

As local authorities should remain close to market participants, we support the proposal to report incidents on a local level. Overall, the EU should have clear, resilient, and proportionate ICT cybersecurity rules.

We agree that templates and formats need to be harmonised and support the approach taken in Art. 18. Furthermore, regulators across multiple jurisdictions should work to harmonise their testing requirements (such as threat-led penetration testing), and then develop principles and requirements that firms should meet when conducting such tests.

It should be left to the firms to conduct the tests, whereas regulators should ensure that their principles are met and that findings are remediated promptly, without having to be involved in every phase of the testing.

Specific exit plans and timelines should be considered per service: DORA gives national financial regulators the power to require customers to temporarily suspend or discontinue the use of ICT provider (Art. 37 (3)). As drafted, and in the context of cloud, this provision could have major impact on EU financial firms, whose business models are based on their ability to build services on the cloud and for whom a sudden request to discontinue use of their preferred ICT provider might be a major business disruption. Further, the threat of suspension and termination of contracts would be a disincentive for EU firms' digitalization efforts, as it would add uncertainty to their investment decisions. Therefore, we recommend to amend the article to consider specific exit plans and timelines per service, ensuring a safe and reasonable transition of a service before it is suspended.

Threat-led penetration tests should explicitly be allowed to also be performed by the financial entity itself: We appreciate that testing methods like "penetration testing" and "red team testing" are foreseen in the proposal. However, from our point of view, it should be explicitly be allowed for a financial entity to perform e.g. thread lead penetration tests by itself, if certain criteria are met (e.g. Art. 23, 24 a) and b)).

As financial entities´ IT architectures are very heterogenous and sometimes very complex, it would be very inefficient to rely solely on external service providers. Also, such requirements might not be possible to fulfill in every case, due to a lack of appropriate external providers. This holds also true for other advanced security testing methods. From our understanding of the proposal, the European Commission does not explicitly forbid firms to use their internal resource to test their systems themselves, but we kindly ask the European Commission to explicitly allow for it and define the terms and conditions.

In this context, we would encourage the European Commission to clarify that the DORA testing regime does not come in addition to and is not independent from the requirements on advanced testing included in the existing frameworks such as the TIBER-EU framework. This would help avoiding any additional compliance costs that firms would incur as a consequence of having to fulfil duplicative requirements on testing.

We believe that, ideally, DORA should state the requirements on how testing should be performed, and then it would be up to regulated entities to conduct the testing, with regulators having the right to review findings – if they wish to do so – and track remediation. This is what, for instance, the CFTC Systems Safeguards Regulation mandates.

IT Asset Management procedures seem appropriate: We appreciate the suggestions made in the proposal, Art. 7 (4) and (7), as they would be compatible with our existing IT asset management procedures.

Proportionality and risk-based approach necessary to define penalties and measures on breaches: We would encourage the European Commission to take into consideration the proportionality and a risk-based approach of breaches before imposing some of the penalties and remedial measures (Art. 44), e.g. the issue of "public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach" (Art. 44 (4) e).