Verband der Auslandsbanken in Deutschland e.V.
Association of Foreign Banks in Germany

European Commission
Directorate-General for Communications,
Networks, Content and Technology
Cybersecurity & Digital Privacy Policy (Unit H.2)
1049 Bruxelles/Brussel
Belgium

18 March 2021

Cybersecurity – review of EU rules on the security of network and information systems: Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020)823

Dear Sir or Madam,

We highly appreciate the opportunity to provide input to the review of the EU rules on the security of network and information systems.

The Association of Foreign Banks in Germany represents the interests of currently more than 200 foreign banks and other financial services institutions which operate in Germany via subsidiary or branch. Almost all member institutions are therefore part of a cross-border banking group. Those banking groups benefit from the regulatory level playing field arising from the harmonisation of financial sector regulations within the European Union.

The proposal of a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, aims at introducing a higher level of harmonisation of security and reporting obligations on European level. We generally support this as it would decrease compliance burden, specifically for entities providing cross-border services. Besides this, the draft Directive aims at replacing the Member States' identification procedures for operators of essential services with a generally applicable obligation and therewith extends the scope of application of this new legislation. With respect to its scope and further issues, we would like to propose the following amendments to the draft Directive:

(A) Classification of small and non-complex credit institutions as important entities according to Annex 2

Regarding the entities in scope of the draft Directive, there is only a differentiation between essential entities (acc. to Annex 1) and important

Andreas Kastl

Association of Foreign Banks in Germany
Weißfrauenstraße 12-16
60311 Frankfurt am Main
Germany
Tel: +49 69 975850 0
Fax: +49 69 975850 10
andreas.kastl@vab.de
www.vab.de

entities (acc. to Annex 2), into which all relevant sectors of the economy are split. In the case of the banking sector (Annex 1 no. 3), all credit institutions referred to in Art. 4 para. 1 no. 1 of Regulation (EU) No. 575/2013 (so-called CRR credit institutions) within the European Union are deemed as essential entities, without acknowledging the vast differences in their sizes, business models and client structures.

With regards to proportionality, the proposal only foresees a general exclusion of micro and small entities from its scope. But considering the magnitude of regulatory requirements banks are subject to, it is hard to believe that any CRR credit institution could benefit from this exclusion, as at least the definition of small enterprises is limited to enterprises which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million according to Art. 2 para. 2 of the Annex of the Recommendation of 6 May 2003, C(2003) 1422.

As the draft Directive aims at establishing a lighter ex-post supervisory regime applied to the important entities (acc. to Annex 2), we would suggest in terms of a more proportionate approach, to list the banking sector also in Annex 2 and treat them as important entities; for purposes of Annex 2, reference should then be made to those CRR credit institutions that are regulated as '**small and non-complex institutions**' acc. to Art. 4 para. 1 no. 145 of Regulation (EU) No. 575/2013 (as amended by Regulation (EU) 2019/876, so-called CRR2). This would allow for a more proportionate regulation in terms of the draft Directive of those credit institutions that fulfil all requirements that are set out in Art. 4 para. 1 no. 145 CRR.

(B) Reference to DORA in order to increase legal certainty

However, we welcome the provisions in the proposal that refer to the Commission's proposal for a Regulation on digital operational resilience for the financial sector (COM(2020) 595 final; so-called **DORA**), which according to the introductory part of the draft Directive will be considered as lex specialis to the proposal at hand once both acts have come into force. Special attention should therefore be given to the general statements in recital 13, whereas DORA should not only be considered to be a sector-specific Union legal act in relation to this draft Directive, but also that DORA's provisions relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set up under this Directive. Given these considerations, the articles of the draft Directive do not explicitly mention any superior application of the coming DORA requirements; only Art. 2 para. 6 of the draft Directive does, in a very general manner, set out that relevant provisions of the draft Directive should not apply if there are provisions of sector–specific acts of Union law requiring essential or important entities either to adopt cyber-security risk management measures or to notify incidents or significant cyber threats.

In this context, it is interesting to note that the Commission's draft of a Directive on the resilience of critical entities (COM(2020) 829 final) entails specific reference to DORA in its Art. 7 para. 2. From our point of view, this will lead to more legal certainty to the application of this so-called CIP Directive.

We therefore suggest to include specific reference to DORA not only in Art.2 para. 6 of the draft Directive, but also in the relevant provisions of chapter IV of the draft Directive concerning cybersecurity risk management and reporting:

- Article 17 on Governance,
- Article 18 on Cybersecurity risk management measures, and
- Article 20 on the reporting obligations.

(C) Clarification on the treatment of branches of essential and important entities established in other Member States

In our contribution to the Commission's consultation on the revision of the NIS Directive that ended on 2 October 2020 (Contribution ID: 97c27d22-7e05-4b8b-802c-b38fcdc011bc), we had already advocated for more harmonised regulation on EU level in the case of a company that has been identified in the existing NIS regime as operator of essential services in more than one Member State and in the case of a groups of companies whose (sub)entities have been identified as an operator of essential services in more than one Member State. In this regard, we acknowledge the general statements of recital 63, pursuant to which an entity that provides services in more than one Member State should fall under the separate and concurrent jurisdiction of each of these Member States. It is commendable that in such cases the involved competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions (in connection to the provisions on supervision and enforcement for essential entities in Article 29).

However, with regards to Article 34 on mutual assistance, we have some concerns regarding the draft Directive's approach to an essential or important entity which provides services in more than one Member State: it is stated that also the competent authority of the Member State of the other establishment or of the representative are in scope of mutual assistance. This provision could be understood in a way that also a **branch** of an essential or important entity that has been established in another Member State could be subject to the provisions of this Directive.

As one manifestation of the freedom of establishment (Article 49 TFEU), the banking regulation on European level also governs the setup of branches in other Member States (cf. Art. 33 of Directive 2013/36/EU). With regards to branches of CRR credit institutions that are established in other Member States (than the home Member State), the current legislation concerning operational risks does address IT security on entity level, including all branches, and there is no supervision in this regard by the host Member State. In our contribution to the Commission's consultation on DORA of 15 February 2021 (Feedback reference F1838380), we also advocated for a clarification in Article 2 of the draft of DORA pursuant to which branches of financial entities acc. to Art. 2 para. 2 of the draft of DORA that are established in other Member States shall themselves not be addressed by the DORA requirements. The DORA requirements should be complied with on entity level instead, in line with the regulatory requirements of CRR.

With regards to the draft Directive, we therefore suggest to clarify that branches of CRR credit institutions established in other Member States cannot themselves constitute essential entities acc. to Annex 1 (or important entities acc. to Annex 2).

(D) Maximum amount of penalties

The harmonisation of penalty provisions at European level is to be commended. The penalties imposed by the member states should be effective and dissuasive, yet in particular they must be proportionate. However, the maximum amount should be 2 million Euros instead of 10 million Euros and should also not be related to the annual turnover. Therefore, Art. 31 para. 4 of the draft Directive should me amended respectively, especially by deleting the phrase “or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher”.

We hope to have hereby given constructive input to the review of the EU rules on the security of network and information systems. Please do not hesitate to contact us if you have any questions.

Kind regards

Dr Andreas Prechtel Andreas Kastl