Frankfurt,
4 March 2024

BVI[1] Position on the ESAs' Consultation Paper on

- **Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and**
- **Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat**

We take the opportunity to present our views on the consultation paper of the ESAs related to Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat.

Question 1 *– Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.*

We do not agree with the proposed timelines for reporting of major incidents. In our view, these are too short, especially the 4-hour deadline for the initial notification. We therefore have the following suggestions for improvement and comments:

- **Initial notification:** The reference points for the two periods differ for the initial notification. According to Art. 6(1)(a) of the draft RTS, reports should be submitted within four hours of 'classification' and no later than 24 hours from the time of 'detection' of the incident. In practice, it seems difficult to use and monitor two different points in time for the initial notification. **It would be more pragmatic to only use one timeline based on the internal classification of the ICT-related incident as major, which also considers the time windows for classifying incidents as major in accordance with the new RTS on classification (Article 18 DORA Regulation).** It should also be taken into account that the suggested timelines for initial notifications will be practically challenging in the case of incidents in the ICT provider chain (in the case of outsourcing of ICT services or subcontractor chains) with a significant impact on the financial entity. Here, earlier information obligations of the outsourcing companies or subcontractors and ICT providers would have to be agreed in order to be able to report the incident in good time.

- **Final report:** In the case of ransomware malware, incident investigation can take months; forensic information is regularly not available within the proposed time periods for submitting the respective reports. It would be desirable to specify when the final report is to be submitted in such cases.

[1] BVI represents the interests of the German fund industry at national and international level. The association promotes sensible regulation of the fund business as well as fair competition vis-à-vis policy makers and regulators. Asset managers act as trustees in the sole interest of the investor and are subject to strict regulation. Funds match funding investors and the capital demands of companies and governments, thus fulfilling an important macro-economic function. BVI's 114 members manage assets of some EUR 4 trillion for retail investors, insurance companies, pension and retirement schemes, banks, churches and foundations. With a share of 27%, Germany represents the largest fund market in the EU. BVI's ID number in the EU Transparency Register is 96816064173-47. For more information, please visit www.bvi.de/en.

BVI
Bundesverband Investment und Asset Management e.V.

Contact
Phone +49 69 15 40 90 0
www.bvi.de

BVI Berlin
Unter den Linden 42
10117 Berlin

BVI Brussels
Rue Belliard 15–17
1040 Bruxelles

BVI Frankfurt
Bockenheimer Anlage 15
60322 Frankfurt am Main

Executive Board
Thomas Richter CEO
Rudolf Siebel MD

Question 2 *– Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

We do not agree with the proposed data fields regarding the impact or potential impact of the incident on other financial entities and/or third-party providers (fields 2.8, 2.9 and 2.10). In particular, fields 2.9. and 2.10. of the initial report shall include description of ‚how' the impact is expected on other entities. This information would be not available and very subjective. Therefore, these fields should be deleted and mostly as an alternative, limiting them to report only of 'if' the impact would be expected on other entities without any description of 'how'. As the DORA framework will also provide the supervisory authorities with extensive information on providers and contracts in future, it must be the task of the supervisors to carry out such impact analyses. This task must not be delegated to the financial entities. This applies all the more when the deadlines for submitting reports are so short. Financial entities themselves have enough work to do to assess the impact of a major ICT incident on their own organisation.

Question 3 *– Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

We refer to our answer to question 2. Any impact analyses of the incident on other financial entities and/or third-party providers should be deleted also in the intermediate report.

Question 4 *– Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

We refer to our answer to question 2. Any impact analyses of the incident on other financial entities and/or third-party providers should be deleted also in the final report.

Question 5 *– Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.*

We have no comments on this.

Question 6 *– Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.*

We do not agree with the proposed processes in case of outsourcing of the reporting obligation. **Article 6(2) of the draft ITS** requires the financial entity to notify the competent authority prior to ***any*** notification or reporting where outsourcing arrangements are of long-term or general nature. The required notification of outsourcing of reporting before each individual incident report makes no sense in practice if financial entities have outsourced the reporting obligation to third parties. A one-off notification should suffice. Irrespective of this, the question arises as to whether the mandate of the ESAs even covers these notification obligations in the event of outsourcing. In our view, the sector-specific regulations should apply to the notification obligations in the event of outsourcing.

Question 7: Do you have any further comment you would like to share?

We do not agree that the exceptions for the **weekend and public holiday regulations** (cf. Article 6(2) and (3) of the draft RTS) should not be permitted for the initial notification. This is not practicable, especially for small companies. In particular, the employment contracts would have to be adapted to be available 24 hours a day, including weekends and public holidays. From a practical point of view, the simplifications created for the intermediate and final notifications for the submission of notifications not on weekends and public holidays would then come to nothing, because permanent availability would then be agreed under labour law anyway.

Irrespective of this, according to Art. 6(3) of the draft RTS, the weekend/holiday exemption should not apply if the incident has an impact on another financial company. There is no materiality threshold here. We therefore request that Art. 6(3) of the draft RTS be amended as follows:

> *'(3) Paragraph 2 shall not apply where the major incident has a **material** impact in another Member State or to another financial entity or that the financial entity is a significant credit institution, a financial market infrastructure or a financial entity deemed significant or systemic by the competent authority for the national market. In this case, the financial entities shall apply the time limits set out in paragraphs 1.'*

****