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

EU-Resilienzvorschriften | EU Rules on Resilience

Gesetzgebungsvorschläge zur Behandlung von IKT-Risiken im Finanzsektor

| Legislative proposals concerning the treatment of ICT risks in the financial sector

Die Europäische Kommission hat am 24. September 2020 Entwürfe für eine Verordnung [2020/0266 (COD)] und für eine (Omnibus-)Richtlinie [2020/0268 (COD)] zur Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen im Finanzsektor veröffentlicht.

Der Verordnungsvorschlag sieht bei den erfassten Unternehmen des Finanzsektors einen umfassenden persönlichen Anwendungsbereich in Art. 2 vor, der unter anderem Kreditinstitute, Zahlungsinstitute und Wertpapierfirmen umfasst.

Die Verordnung soll gemäß Art. 1 Abs. 2 als sektorspezifischer Rechtsakt bei den Betreibern kritischer Infrastrukturen des Finanzsektors Vorrang vor den nationalen Bestimmungen zur Umsetzung der NIS-Richtlinie haben (vgl. Art. 1 Abs. 7 NIS-Richtlinie (EU) 2016/1148).

Die Governance-bezogenen Anforderungen in Art. 4 sehen vor, dass das Leitungsorgan der regulierten Einheiten eine entscheidende, aktive Rolle bei der Gestaltung des Rahmenwerks für das IKT-Risikomanagement übernehmen muss. Für alle IKT-bezogenen Funktionen sollen Rollen und Verantwortlichkeiten eindeutig zugewiesen werden.

Nach den Anforderungen zum IKT-Risikomanagement gemäß Art. 5 bis 14 sollen Finanzinstitute unter anderem dazu verpflichtet werden:

- belastbare IKT-Systeme und Tools, die das IKT-Risiko in seinen Auswirkungen minimieren können, einzurichten und beizubehalten,
- kontinuierlich alle Quellen von IKT-Risiken zu identifizieren,
- Schutz- und Präventionsmaßnahmen einzurichten,
- in der Lage zu sein, anomale Aktivitäten sofort zu erkennen, als auch
- dedizierte und umfassende Grundsätze der Geschäftskontinuität, sowie Katastrophen- und Wiederherstellungspläne als integraler Bestandteil der betrieblichen Geschäftskontinuitätspolitik einzuführen.

Darüber hinaus zielen die Anforderungen von Art. 15 bis 20 darauf ab, ein europäisches Rahmenwerk für das Berichtswesen über IKT-bezogene Vorfälle zu etablieren. Das Berichtswesen soll mit einer gemeinsamen Meldevorlage und nach einem harmonisierten Verfahren, das von den ESAs entwickelt werden soll, durchgeführt werden. Hierbei ist anzuerkennen, dass Art. 19 die europäischen Behörden anweist, die Machbarkeit einer einheitlichen Meldestelle bei

On 24 September 2020, the European Commission presented drafts for a Regulation [2020/0266 (COD)] and for an (omnibus) Directive [2020/0268 (COD)] on the improvement of digital operational resilience for the financial sector.

With respect to the encompassed companies of the financial sector, the proposal of the Regulation provides for an extensive personal scope of application that covers inter alia, credit institutions, payment institutions, and investment firms.

According to Art. 1 para. 2 of the Regulation, it shall be considered as a sector-specific legal act in relation to financial entities identified as operators of essential services that takes precedence over the national implementations of the NIS Directive (cf. Art. 1 para. 7 of the NIS Directive (EU) 2016/1148).

The Governance related requirements in Art. 4 stipulate that the management body of regulated entities shall be required to maintain a crucial, active role in steering the ICT risk management framework. There shall be an assignment of clear roles and responsibilities for all ICT-related functions established, too.

According to the ICT risk management requirements as laid down in Art. 5 to 14, financial entities shall – inter alia – be required:

- to set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk,
- to identify on a continuous basis all sources of ICT risk,
- to set-up protection and prevention measures,
- to be able to promptly detect anomalous activities, and
- to put in place dedicated and comprehensive business continuity policies and disaster and recovery plans as an integral part of the operational business continuity policy.

Furthermore, the requirements of Art. 15 to 20 establish a European framework on ICT-related incident reporting by which only ICT-related incidents. The reporting should be processed using a common template and following a harmonised procedure as developed by the ESAs. It has to be acknowledged that Art. 19 instructs the European authorities to assess the feasibility of a single EU Hub for major ICT-related incident reporting by financial entities.

schwerwiegenden IKT-bezogenen Vorfällen durch Finanzinstitute zu prüfen.

Neben den Bestimmungen zum Testen der Widerstandsfähigkeit (Art. 21 bis 24) enthält der Verordnungsentwurf auch regulatorische Anforderungen in Bezug auf das IKT-Risiko bei Drittdienstleistern (Art. 25 bis 39). Dazu gehören auch Anforderungen in Bezug auf die vertraglichen Vereinbarungen, die zwischen IKT-Drittdienstleistern und Finanzinstituten geschlossen werden.

Abschließende Bestimmungen der Verordnung, als auch die vorgeschlagene Richtlinie, dienen der Anpassung bestehender Rechtsakte auf EU-Ebene. Beide Rechtsakte sollen grundsätzlich 12 Monate nach Veröffentlichung im Amtsblatt in Kraft treten.

Insgesamt weisen die Gesetzgebungsvorschläge der Kommission Ähnlichkeiten mit den EBA-Leitlinien zum Management von IKT- und Sicherheitsrisiken vom 28. November 2019 (EBA/GL/2019/04) auf (siehe VAB-Bericht vom 29. November 2019), die in Deutschland im Rahmen der Überarbeitung der bankaufsichtlichen Anforderungen an die IT (BAIT) der BaFin umgesetzt werden sollen (vgl. u. a. VAB-Bericht vom 23. März 2020). Zu beachten ist jedoch, dass die endgültige Verordnung direkt anwendbares Recht in allen Mitgliedstaaten darstellen wird. Die Verordnung ist inhaltlich auch nicht als Ersatz der europäischen NIS-Richtlinie anzusehen. In diesem Zusammenhang sei auch auf die Stellungnahme vom 2. Oktober 2020 verwiesen, mit der sich der Verband an der öffentlichen Konsultation zur Überprüfung der NIS-Richtlinie (siehe VAB-Bericht vom 10. Juli 2020) beteiligt hat.

Der Verband nimmt die Anmerkungen seiner Mitglieder für eine etwaige Rückmeldung an die Kommission gerne bis zum 2. November 2020 entgegen, bestenfalls per E-Mail an andreas.kastl@vab.de.

Besides the provisions on digital operational resilience testing (Art. 21 to 24), the draft regulation also contains regulatory requirements with regards to ICT third-party risk (Art. 25 to 39). This includes also requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities.

The Regulation's concluding provisions as well as the proposed directive provide for necessary amendments to existing legal acts on EU level. Both legal acts have in common a general entry into force 12 months after publication in the EU Official Journal.

Overall, the Commission's legislative proposals show similarities with the EBA Guidelines on ICT and security risk management of 28 November 2019 (EBA/GL/2019/04) (see VAB report of 29 November 2019), which are to be implemented in Germany within the framework of the revision of the prudential requirements for IT (BAIT) originated by BaFin (see inter alia VAB report of 23 March 2020). However, it should be noted that the final Regulation will become directly applicable law in all Member States. The Regulation should not be seen as a replacement for the European NIS Directive either. In this context, we refer to the position paper of 2 October 2020 with which the Association participated in the public consultation on the review of the NIS Directive (see VAB report of 10 July 2020).

The Association welcomes the comments of its members for eventual feedback to the Commission by 2 November 2020, at best via e-mail to andreas.kastl@vab.de.

Kontakt: | Contact:

Andreas Kastl
andreas.kastl@vab.de

Andreas Kastl, M.A., LL.M.oec.
Abteilungsdirektor Bankinfrastruktur | Department Head Bank Infrastructure
Verband der Auslandsbanken in Deutschland e.V. | Association of Foreign Banks in Germany
Weißfrauenstraße 12-16, D-60311 Frankfurt am Main | Fon +49 69 975850-0 | Fax +49 69 975850-10
andreas.kastl@vab.de | www.vab.de
Eingetragen im Vereinsregister des Amtsgerichts Frankfurt am Main: VR 7860
Impressum
Datenschutz