GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Inhalt

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Betriebswirtschaft, IT und Prozesse

E-Mail
bdit@gdv.de

Zusammenfassung

Die deutsche Versicherungswirtschaft als Teil der Kritischen Infrastruktur Deutschlands unterstützt das Vorhaben des Bundesinnenministeriums, die Cyberresilienz in Deutschland als Teil des europäischen Raums weiter zu stärken. Auch wenn Versicherungsunternehmen von der NIS-2-Richtlinie und deren nationaler Umsetzung grundsätzlich nicht erfasst werden, nehmen wir die Gelegenheit zur Stellungnahme gerne wahr, da Teile einer Versicherungskonzernstruktur doch in den Anwendungsbereich fallen sollen. Darüber hinaus ist die Umsetzung der Richtlinien-Vorgaben zur Geschäftsleiterhaftung relevant für das Geschäftsfeld der D&O-Versicherer.

1. Einleitung

Durch den Digital Operational Resilience Act (DORA: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor) unterliegen Versicherungsunternehmen bereits umfassenden Vorgaben – z. B. Melde- und Nachweispflichten. Zur Vermeidung von Doppelregulierung hat der Europäische Gesetzgeber daher eine lex-specialis-Regelung in DORA aufgenommen. Die Versicherungsunternehmen sollen als Finanzunternehmen im Sinne von Artikel 2 Absatz 2 der DORA-Verordnung entsprechend von NIS2 ausgenommen sein.

Allerdings gilt dies nach dem definierten Anwendungsbereich nicht für deren gruppeninternen IT-Töchter. Wenn diese jedoch ausschließlich für eines bzw. mehrere der aus dem Anwendungsbereich ausgenommenen Versicherungsunternehmen IKT-Dienstleistungen erbringen, ist eine Regulierung über das NIS-2-Umsetzungsgesetz neben DORA nicht erforderlich.

1.1 Zu § 28 BSI-Gesetz (Besonders wichtige und wichtige Einrichtungen): Besonderheit der unternehmenseigenen bzw. gruppeninternen IT-Dienstleister in der Versicherungswirtschaft

Im Referentenentwurf zum NIS-2-Umsetzungsgesetz wird in Kapitel 1 „Anwendungsbereich in § 28 „Besonders wichtige Einrichtungen und wichtige Einrichtungen“ die Versicherungswirtschaft über die Nennung von DORA als lex specialis ausgenommen. Der hier einschlägig zitierte Artikel 2 Abs. 2 benennt die Unternehmen als Finanzunternehmen, für die alle Bestimmungen aus DORA gelten. In diesem Artikel ausgenommen sind die IKT-Drittanbieter, die damit auch unter die NIS-2 und das entsprechende Umsetzungsgesetz fallen würden. Sinnvoll wäre eine generelle Ausnahme für alle Unternehmen des Finanzsektors, die DORA unterliegen. Zumindest solche IKT-Drittdienstleister, die ausschließlich gruppenintern tätig sind, sollten ebenfalls aus dem Anwendungsbereich des NIS-2-Umsetzungs-

gesetzes herausgenommen werden. Diese Wertung entspräche auch dem Verständnis des Europäische Gesetzgebers, der gruppeninterne IKT-Drittdienstleister von dem Überwachungsrahmen für kritische IKT-Drittanbieter nach DORA ausnimmt. Dies trägt dem Umstand Rechnung, dass die stark regulierten Finanzunternehmen regelmäßig größeren Einfluss auf die gruppeninternen Dienstleister haben und die Einhaltung der strengen Sicherheitsanforderungen bereits hinreichend überwachen.

Eine Einbeziehung von gruppeninternen Dienstleistern, die ausschließlich IT-Dienstleistungen an regulierte Unternehmen anbieten, die aufgrund der hohen Sicherheitsanforderungen nach DORA selbst nicht unter das NIS-2-Umsetzungsgesetz fallen, erscheint zudem ohne besonderen Mehrwert. Es stellt sich die Frage, welchen erhöhten Risiken solche Unternehmen im Gegensatz zu IT-Abteilungen innerhalb eines Versicherungsunternehmens (In-House) ausgesetzt sind. Aus unserer Sicht rechtfertigt dies im Ergebnis keine Doppelregulierung durch DORA und NIS-2. Wir regen die Streichung der gruppeninternen Dienstleister aus dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes an:

§28 Abs (5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für
1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für welche die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 Kreditwesengesetz oder § 293 Absatz 5 Versicherungsaufsichtsgesetz gelten, *sowie deren gruppeninternen IKT-Dienstleister.*

1.2 Zu § 38 BSI-Gesetz (Geschäftsleiterhaftung)

Wir begrüßen die erkennbaren Verbesserungen in der Ausgestaltung von § 38 Abs. 2 BSIG-E im Vergleich zu der noch in dem Diskussionspapier enthaltenen Formulierung. Anstelle eines generellen Vergleichsverbots wird nun klargestellt, dass dieses zwar Beschränkungen unterliegen soll, aber grundsätzlich zulässig bleibt. Hilfreich ist hierbei auch die Erläuterung in der Begründung, insbesondere die Klarstellung, dass der Abschluss einer D&O-Versicherung weiterhin möglich bleibt. Gleichwohl erlauben wir uns an dieser Stelle noch einmal darzulegen, weshalb wir im Ergebnis eine **gänzliche Streichung von § 38 Absatz 2 BSIG-E** für angebracht halten.

Wenngleich § 38 Absatz 2 BSIG-E einen den Rechtsrisiken angemessenen Vergleich grundsätzlich zulässt, bleiben für die Praxis Unsicherheiten bei der Auslegung bestehen. Die Gesetzesbegründung bietet hier zwar eine gewisse Orientierung, indem klargestellt wird, dass ein Vergleich unzulässig ist, wenn das Entgegenkommen der Einrichtung „gemessen an den jeweiligen prozessualen Risiken grob unverhältnismäßig ist“ und dass bei gerichtlich vorgeschlagenen Vergleichen grundsätzlich von einem angemessenen Verhältnis auszugehen ist. Dennoch verbleiben gerade für den in Organhaftungsfällen praktisch sehr bedeutsamen

Bereich außergerichtlicher Vergleiche nicht unerhebliche Unsicherheiten, die durch eine Streichung von § 38 Abs. 2 BSIG-E beseitigt würden.

Eine Streichung wäre aus unserer Sicht auch mit Art. 20 Abs. 1 NIS-2-Richtlinie vereinbar, wonach die Mitgliedstaaten sicherzustellen haben, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen für Verstöße gegen die in Artikel 21 genannten Risikomanagementmaßnahmen durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Die Gesetzesbegründung zu § 38 Abs. 2 BSIG-E führt zutreffend aus, dass sich die Binnenhaftung der Leitungsorgane bei Verletzung von Pflichten nach dem BSIG bereits aus den allgemeinen gesellschaftsrechtlichen Haftungsregelungen (z. B. § 93 AktG, § 43 GmbHG) ergibt. Dementsprechend entstünde bei einer Streichung kein haftungsfreier Raum. Ebenso wenig wäre die Haftung frei disponibel. Bei Aktiengesellschaften ist ein Vergleich oder Verzicht z. B. nur unter Beachtung der strengen Voraussetzungen des § 93 Abs. 4 AktG, insbesondere der Zustimmung der Hauptversammlung, möglich.

Die Streichung bereichsspezifischer Haftungsregelungen würde auch der Einheit der Rechtsordnung dienen und Wertungswidersprüche zu den allgemeinen gesellschaftsrechtlichen Haftungsnormen vermeiden.

Berlin, den 28.05.2024