GDV Gesamtverband der Versicherer

**Entwurf eines Gesetzes über die Digitalisierung des Finanzmarktes**
(Finanzmarktdigitalisierungsgesetz – FinmadiG)

Der Regierungsentwurf zum Finanzmarktdigitalisierungsgesetz soll unter anderem die erforderlichen nationalen Anpassungen zur Durchführung des Digital Operational Resilience Act (DORA) vornehmen. Durch die Erweiterung des Abschlussprüfermandats auf nahezu alle DORA-Vorgaben sowie die Einbeziehung von Versicherungs-Holdinggesellschaften schießt der Gesetzentwurf über das Ziel hinaus. Aus nachfolgenden Erwägungen sollten die Vorschläge gestrichen werden.

## I. Keine Ausdehnung des Abschlussprüfermandats

Der Gesetzentwurf weitet in Art. 11 Nr. 2 das Mandat der Abschlussprüfer auf sämtliche unternehmensrelevante Vorgaben des neuen „Digital Operational Resilience Act“(DORA) aus. Abschluss-prüfer sollen künftig prüfen, ob die Versicherungsunternehmen eine gesetzeskonforme Resilienz im Bereich der Informations- und Kommunikationstechnologie (IKT) implementiert haben. Da der Gesetzentwurf keinerlei Beschränkung auf abschlussprüfungsrelevante Sachverhalte wie etwa IKT-Buchhaltungs- und Bilanzierungstools vorsieht, umfasst die Prüfung sämtliche IKT-Prozesse, IKT-Systeme und IKT-Anwendungen eines Unternehmens, beispielsweise Kundenverwaltungs-systeme, Vertragsdatenbanken oder Schadenbearbeitungstools. Eine solch weitgehende Prüfung steht in keinem erkennbaren Zusammenhang mehr zu den Aufgaben der Abschlussprüfung und führt zu erheblich höheren Kosten für die Unternehmen und letztlich für die Versicherungskunden. Dies widerspricht der aktuellen Initiative zum Bürokratieabbau der Bundesregierung. Die externe Prüfung ist zudem völlig redundant, setzt DORA doch gerade mit dem Modell der drei Verteidigungslinien einschließlich unabhängiger IKT-Risikomanagementfunktion und unabhängiger IKT-Revision auf eine umfassende interne Risikoüberwachung. Unabhängig davon ist die fachliche Eignung von Jahresabschlussprüfern zu hinterfragen, wenn es etwa um die Prüfung der Angemessenheit von Schwachstellenscans, Open-Source-Analysen, Netzwerksicherheitsbewertungen oder Quellcodeprüfungen geht. Es ist jedenfalls davon auszugehen, dass viele kleine und mittlere Wirtschaftsprüfungsgesellschaften dies nicht abdecken werden können, was zu einer weiteren Markt-konzentration der Abschlussprüferleistungen im Versicherungsbereich führen dürfte.

## II. Einbeziehung von Versicherungs-Holdinggesellschaften

Über die europäischen Vorgaben hinaus unterwirft der Gesetzentwurf in Art. 11 Nr. 3 Versicherungs-Holdinggesellschaften und Unternehmen nach § 293 Abs. 4 VAG zusätzlich den strengen DORA-Anforderungen, obwohl diese selbst keine Risikoträger sind. Der Erwerb und das Halten von Beteiligungen sind rein wirtschaftliche Beziehungen ohne Übernahme von oder Auswirkungen auf die IT-Risiken. Diese nationale Ausdehnung auch auf Nicht-Risikoträger geht an dem erklärten Ziel von DORA, das Finanzsystem stärker vor Cyberrisiken und dadurch verbundene Ausfälle zu schützen, vorbei. IT-Beeinträchtigungen der Holding strahlen gerade nicht auf die zugehörigen eigenständig operierenden Risikoträger aus. Dem Verbraucher respektive Versicherungsnehmer drohen mithin keine negativen Folgen der Beeinträchtigung der Holding. Sofern Holdings selbst auch das Versicherungsgeschäft betreiben oder als IT-Dienstleister für die Risikoträger auftreten –und damit ein Risikopotenzial besteht - unterfallen diese schon jetzt DORA. Somit besteht keine zu schließende Schutzlücke. Dem Mehraufwand steht kein entsprechender Mehrwert gegenüber.