8. Jahrgang / März 2026 / Nr. 2

ZVers

Zeitschrift für Versicherungsrecht

Erwin Gisch | Michael Gruber | Felix Hörlsberger | Walter Kath | Martin Ramharter

Linde
www.lindeverlag.at

DORA und NISG 2026: Implikationen für Versicherer und Versicherungsnehmer

Felix Schneider / Christopher Drolz

Das am 23. 12. 2025 im BGBl I 2025/94 kundgemachte Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) setzt die europäische NIS-2-Richtlinie[1] in österreichisches Recht um und verpflichtet die darin definierten wesentlichen und wichtigen Einrichtungen zur Umsetzung umfassender Cybersicherheitsmaßnahmen. Für einen Großteil der Versicherungs- und Rückversicherungsunternehmen gilt jedoch der Anwendungsvorrang der DORA,[2] weshalb das NISG 2026 auf sie nicht unmittelbar anwendbar ist. Gleichwohl kommt dem Gesetz auch für die Versicherungsbranche erhebliche Bedeutung zu; insbesondere können im relevanten Kontext tätige IKT-Drittdienstleister[3] beiden Regelungsregimen unterliegen und die neuen Pflichten des NISG 2026 sind geeignet, sich auf vertragliche Obliegenheiten, Risikoausschlüsse sowie die Prämiengestaltung auszuwirken.

Mag. Felix Schneider ist Rechtsanwalt bei Schönherr Rechtsanwälte in Wien.

Christopher Drolz, LL.M. (WU), MBA, CIPP/E ist Rechtsanwalt bei Schönherr Rechtsanwälte in Wien.

1. Allgemeines zum NISG 2026

Das NISG 2026 ist ein grundlegender Meilenstein in der österreichischen Cybersicherheitsarchitektur. Es setzt die NIS-2-Richtlinie in nationales Recht um.

Primäres Ziel des NISG 2026 ist die Gewährleistung eines hohen Cybersicherheitsniveaus für wesentliche und wichtige Einrichtungen. Das Gesetz tritt neun Monate nach seiner Kundmachung mit dem nächstfolgenden Monatsersten, somit am 1. 10. 2026, in Kraft.

Für die erfassten Unternehmen und Organisationen begründet das NISG 2026 umfassende Pflichten insbesondere in den Bereichen Risikomanagement, Meldewesen und Governance, deren Einhaltung durch ein abgestuftes Sanktionsregime abgesichert wird.

Besondere praktische Relevanz kommt dem Verhältnis zur DORA zu. Für Einrichtungen, die dem Anwendungsbereich der DORA unterliegen (darunter befinden sich gemäß Art 2 Abs 1 lit n DORA ausdrücklich bestimmte Versicherungs- und Rückversicherungsunternehmen), ordnet § 24 Abs 7 NISG 2026 den Vorrang der sektorspezifischen Regelung an.

2. Grundlegende Ziele und Regelungszweck

Das NISG 2026 verfolgt einen umfassenden regulatorischen Ansatz zur Stärkung der Cybersicherheit in Österreich. Diese Zielsetzung manifestiert sich in der systematischen Erfassung kritischer Sektoren, die in § 2 NISG 2026 aufgezählt sind. Das erfasste Spektrum reicht von klassischen kritischen Infrastrukturen (wie Energie, Verkehr und Gesundheitswesen) bis hin zu digitalen Bereichen (insbesondere zu IKT-Diensten).

Der Regelungsansatz des NISG 2026 beruht auf einem gefahrenübergreifenden Verständnis von Cybersicherheit, das technische, organisatorische und operative Aspekte gleichermaßen erfasst. Cybersicherheit wird dabei als Schutz von Netz- und Informationssystemen, der Nutzer solcher Systeme sowie sonstiger von Cyberbedrohungen betroffener Personen definiert (§ 3 Z 3 NISG 2026). Dieser weite Schutzzweck findet seinen Ausdruck in den umfassenden Pflichten, die das Gesetz (insbesondere §§ 29 ff NISG 2026) den betroffenen Einrichtungen auferlegt. Zugleich verfolgt das NISG 2026 einen risikobasierten Ansatz: Art und Intensität der zu treffenden Maßnahmen richten sich nach der jeweiligen Risikoexposition, der Größe der Einrichtung sowie nach der Wahrscheinlichkeit und Schwere potenzieller Sicherheitsvorfälle.

Besondere Bedeutung kommt schließlich der institutionellen Neuordnung zu. Mit der Errichtung des Bundesamtes für Cybersicherheit (Cybersicherheitsbehörde) als unmittelbar dem BMI nachgeordnete Behörde wird eine zentrale Anlaufstelle für Cybersicherheitsfragen geschaffen. Die organisatorische Verortung außerhalb der Generaldirektion für die öffentliche Sicherheit unterstreicht die institutionelle Eigenständigkeit der Behörde. Weisungen des Bundesministers sind schriftlich zu erteilen, zu begründen und halbjährlich zu veröffentlichen, um ein hohes Maß an Transparenz sicherzustellen.

3. Anwendungsbereich und zentrale Definition

Der sachliche Anwendungsbereich des NISG 2026 erstreckt sich auf 18 explizit benannte Sektoren

---

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. 12. 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl L 333 vom 27. 12. 2022, S 80.

2 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. 12. 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr 1060/2009, (EU) Nr 648/2012, (EU) Nr 600/2014, (EU) Nr 909/2014 und (EU) 2016/1011, ABl L 333 vom 27. 12. 2022, S 1.

3 Das Kürzel „*IKT*" steht für Informations- und Kommunikationstechnologie.

samt ihren Teilsektoren gemäß den Anlagen 1 und 2. Damit weist das NISG 2026 im Vergleich zum bisherigen NISG 2018 einen deutlich erweiterten Anwendungsbereich auf.

Zentrales Strukturmerkmal des Gesetzes ist die Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen, die erhebliche Auswirkungen sowohl auf die Intensität der behördlichen Aufsicht als auch auf die Höhe der vorgesehenen Sanktionen hat. Als wesentliche Einrichtungen gelten unabhängig von der Unternehmensgröße etwa qualifizierte Vertrauensdiensteanbieter, von der Cybersicherheitsbehörde als wesentlich eingestufte Einrichtungen sowie Einrichtungen, die als kritische Einrichtungen im Sinne der RKE-Richtlinie[4] ermittelt wurden.[5] Darüber hinaus zählen zu den wesentlichen Einrichtungen mittlere Unternehmen, die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste sind, sowie große Unternehmen, die den in Anlage 1 zum NISG 2026 genannten Sektoren angehören. Die als wichtige Einrichtungen erfassten Einrichtungen sind demgegenüber in § 24 Abs 2 NISG 2026 taxativ angeführt.

Die Größenbestimmung orientiert sich an den Kriterien der Empfehlung 2003/361/EG.[6] Ein großes Unternehmen liegt nach § 25 Abs 2 NISG 2026 vor, wenn es zumindest 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von mehr als 50 Mio € erzielt und zugleich eine Jahresbilanzsumme von über 43 Mio € aufweist. Als mittleres Unternehmen gilt hingegen eine Einrichtung, die zumindest 50 Mitarbeiter beschäftigt oder einen Jahresumsatz von mehr als 10 Mio € erzielt und eine Jahresbilanzsumme von über 10 Mio € aufweist, sofern sie nicht bereits als großes Unternehmen einzustufen ist.

Diese größenabhängige Differenzierung wird durch die Möglichkeit der Cybersicherheitsbehörde ergänzt, auch kleinere Einrichtungen, die Tätigkeiten gemäß Anlage 1 oder 2 zum NISG 2026 erbringen, per Bescheid als wesentlich oder wichtig einzustufen, etwa wenn sie der einzige Anbieter eines für kritische Tätigkeiten unerlässlichen Dienstes sind oder wenn eine Störung ihrer Dienste erhebliche Auswirkungen auf die öffentliche Ordnung, Sicherheit oder Gesundheit haben könnte (§ 26 NISG 2026).

4. Kernpflichten für wesentliche und wichtige Einrichtungen

4.1. Vorbemerkung

Das NISG 2026 etabliert ein im Wesentlichen dreistufiges Pflichtenprogramm: Governance-Anforderungen, Risikomanagementmaßnahmen und Meldepflichten, die aufeinander abgestimmt sind.

4.2. Governance-Pflichten der Leitungsorgane

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen tragen eine besondere Verantwortung für die Cybersicherheit (§ 31 NISG 2026). Sie haben die Einhaltung der Risikomanagementmaßnahmen sicherzustellen und zu beaufsichtigen. Diese Überwachungspflicht begründet eine persönliche Verantwortung der Geschäftsleitung. Darüber hinaus müssen die Leitungsorgane an spezifisch für sie konzipierten Cybersicherheitsschulungen teilnehmen. Die Einrichtungen sind zudem verpflichtet, ihren Mitarbeitenden entsprechende Schulungen anzubieten, sodass diese über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um Risiken zu erkennen, zu bewerten und Managementpraktiken im Bereich der Cybersicherheit sowie deren Auswirkungen wirksam umzusetzen. Diese Anforderungen verdeutlichen den ganzheitlichen Ansatz des NISG 2026, der Cybersicherheit als organisationsweite Verantwortung versteht und sich nicht auf die IT-Abteilung beschränkt.

4.3. Risikomanagementmaßnahmen im Bereich der Cybersicherheit

§ 32 NISG 2026 normiert umfassende Risikomanagementpflichten, die das Kernstück der materiellen Anforderungen des Gesetzes bilden. Wesentliche und wichtige Einrichtungen sind verpflichtet, geeignete und verhältnismäßige Maßnahmen in technischer, organisatorischer und operativer Hinsicht umzusetzen.[7]

Der Gesetzgeber betont die Verhältnismäßigkeit: Das zu gewährleistende Sicherheitsniveau muss dem jeweiligen Risiko angemessen sein und dabei den Stand der Technik, die einschlägigen Normen, die bewährten Verfahren sowie die entstehenden Kosten berücksichtigen (§ 32 NISG 2026).

Die erforderlichen Maßnahmen werden in einem detaillierten Katalog konkretisiert, der einem gefahrenübergreifenden Ansatz folgt (§ 32 Abs 4 NISG 2026).[8] Dieser Katalog umfasst etwa:

- Konzepte bezüglich Risikoanalyse und Informationssystemsicherheit;
- Maßnahmen zur Bewältigung von Cybersicherheitsvorfällen;
- Vorkehrungen zur Aufrechterhaltung des Betriebs einschließlich Back-up-Management;
- Wiederherstellung nach einem Notfall und Krisenmanagement.

Besonderes Gewicht misst das Gesetz der Sicherheit der Lieferkette bei, wobei die spezifischen Schwachstellen der unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und die Cybersicherheitspraxis zu berücksichtigen sind.

4.4. Nachweis- und Registrierungspflichten

Das NISG 2026 sieht in § 33 ein gestuftes Nachweissystem vor:

Wesentliche und wichtige Einrichtungen müssen der Cybersicherheitsbehörde bis spätestens 30. 9. 2027 eine Selbstdeklaration übermitteln (§ 33 Abs 1 NISG 2026). Diese muss Informationen über die umgesetzten Risikomanagementmaßnahmen enthalten (insbesondere betreffend die genutzten Netz- und Informationssysteme, die Sicherheit der Lieferketten sowie die Ergebnisse der durchgeführten Risikoanalyse). Darüber hinaus haben die Einrichtungen innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde die Umsetzung der Risikomanage-

4 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. 12. 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl L 333 vom 27. 12. 2022, S 164.

5 Diese Richtlinie wurde in Österreich im am 16. 10. 2025 im BGBl I 2025/60 veröffentlichten RKEG umgesetzt.

6 Empfehlung der Kommission vom 6. 5. 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 124 vom 20. 5. 2003, S 36.

7 Weiterführend *Drolz*, Mögliche Konsequenzen sowie Prävention eines Cyber-Vorfalls, GRC aktuell 2023, 49.

8 Für bestimmte Einrichtungen existiert ein noch detaillierterer Katalog des europäischen Gesetzgebers in der Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. 10. 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, ABl L 2024/2690 vom 18. 10. 2024, S 1.

mentmaßnahmen durch eine von einer unabhängigen Stelle sowie auf Basis einer Risikoanalyse bzw sonstigen Risikoabwägung durchgeführten Prüfung nachzuweisen. Für wesentliche Einrichtungen gilt hinsichtlich der operativen und organisatorischen Umsetzung eine verkürzte Nachweisfrist von zwei Monaten. Die erstmalige Aufforderung kann frühestens nach Ablauf von zwei Jahren ab Inkrafttreten des Gesetzes, also frühestens ab 1. 10. 2028, erfolgen (§ 33 Abs 2 NISG 2026).

Betroffene Einrichtungen müssen sich zudem bei der Cybersicherheitsbehörde registrieren und dabei strukturierte Angaben übermitteln (§ 29 NISG 2026). Dazu zählen unter anderem der Name und die Anschrift der Einrichtung, Kontaktdaten, der Sektor oder die Sektoren, die Art der Einrichtung, die Mitgliedstaaten, in denen Dienste erbracht werden, gegebenenfalls IP-Adressbereiche, die Anschrift der Hauptniederlassung sowie Angaben zur Unternehmensgröße. Die Registrierung ist innerhalb von drei Monaten nach Inkrafttreten des Gesetzes vorzunehmen, das heißt spätestens am 31. 12. 2026; Einrichtungen, die die Voraussetzungen erst später erfüllen, haben eine Frist von drei Monaten ab Erfüllung der jeweiligen Voraussetzungen (§ 29 Abs 3 NISG 2026).

4.5. Melde- und Berichtspflichten

Das Meldewesen des NISG 2026 ist als mehrstufiges Verfahren ausgestaltet (§§ 34 und 35 NISG 2026). Wesentliche und wichtige Einrichtungen sind verpflichtet, jeden erheblichen Cybersicherheitsvorfall dem für sie zuständigen sektorspezifischen Computer-Notfallteam (*computer security incident response team* – CSIRT) oder – sofern ein solches nicht eingerichtet ist – dem nationalen CSIRT zu melden. Ein Cybersicherheitsvorfall gilt *ex lege* als erheblich, wenn er entweder schwerwiegende Betriebsstörungen der erbrachten Dienste der Einrichtung verursacht oder verursachen könnte oder wenn er zu erheblichen finanziellen Verlusten für die betroffene Einrichtung führt oder führen könnte. Außerdem wird ein Cybersicherheitsvorfall als erheblich eingestuft, wenn dadurch andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt sind oder sein könnten.

Das gestufte Meldeverfahren beginnt mit einer Frühwarnung, die unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung des Vorfalls zu übermitteln ist. Soweit relevant, ist in der Frühwarnung anzugeben, ob der Verdacht besteht, dass der Vorfall auf rechtswidrige oder schuldhafte Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte.

Innerhalb von 72 Stunden nach Bekanntwerden ist eine weiterführende Meldung über den Cybersicherheitsvorfall zu erstatten,[9] die etwa eine erste Bewertung des Vorfalls (insbesondere seines Schweregrads und seiner Auswirkungen) sowie gegebenenfalls Kompromittierungsindikatoren zu enthalten hat. Auf Anforderung sind Zwischenberichte vorzulegen. Spätestens einen Monat nach der Erstmeldung ist ein Abschlussbericht vorzulegen,[10] der unter anderem eine ausführliche Darstellung des Vorfalls, Angaben zur Art der Bedrohung sowie zu den zugrunde liegenden Ursachen umfasst. Beeinträchtigt ein erheblicher Cybersicherheitsvorfall die Erbringung des jeweiligen Dienstes, hat die betroffene Einrichtung darüber hinaus die Empfänger ihrer Dienste unverzüglich über den Vorfall zu informieren und Maßnahmen oder Abhilfemaßnahmen mitzuteilen.

[9] Für bestimmte Einrichtungen ist diese Frist auf 24 Stunden verkürzt; vgl § 34 Abs 2 NISG 2026.

[10] Sofern der Vorfall noch andauert, bestehen Sonderregelungen gemäß § 34 Abs 2 Z 5 NISG 2026.

5. Sanktionsregime und behördliche Durchsetzung

5.1. Verwaltungsstrafbestimmungen

Die Verwaltungsstrafbestimmungen des § 45 NISG 2026 knüpfen an unterschiedliche Pflichtverletzungen an und staffeln das Sanktionsniveau nach der Einstufung der betroffenen Einrichtung. Verstößt eine wesentliche Einrichtung gegen zentrale Verpflichtungen (etwa gegen die Umsetzung der vorgeschriebenen Risikomanagementmaßnahmen oder die fristgerechte Meldung erheblicher Cybersicherheitsvorfälle), drohen Geldstrafen von bis zu 10 Mio € oder bis zu 2 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, wobei jeweils der höhere Betrag maßgeblich ist.

Für wichtige Einrichtungen liegt die entsprechende Obergrenze bei 7 Mio € oder 1,4 % des weltweiten Vorjahresumsatzes.

Für weniger schwerwiegende Verstöße (etwa die nicht fristgerechte Erfüllung der Registrierungspflicht) sieht das Gesetz Geldstrafen von bis zu 50.000 € und im Wiederholungsfall von bis zu 100.000 € vor.

5.2. Aufsichts- und Durchsetzungsmaßnahmen

Die Cybersicherheitsbehörde ist mit weitreichenden Aufsichts- und Durchsetzungsbefugnissen ausgestattet (§§ 38 und 39 NISG 2026). Zu den Aufsichtsmaßnahmen gegenüber wesentlichen Einrichtungen zählen insbesondere Kontrollen vor Ort und aus der Ferne, die Durchführung von Sicherheitsscans, die Anforderung von Informationen zur Bewertung der umgesetzten Risikomanagementmaßnahmen sowie die Vornahme anlassbezogener *Ad-hoc*-Prüfungen. Viele dieser Maßnahmen können auch gegenüber wichtigen Einrichtungen angewendet werden (§ 38 Abs 2 NISG 2026).

Das Spektrum der Durchsetzungsmaßnahmen reicht von der Anordnung konkreter Maßnahmen über die öffentliche Bekanntmachung von Verstößen bis hin zur Bestellung eines Überwachungsbeauftragten, der für einen bestimmten Zeitraum die Einhaltung der gesetzlichen Anforderungen sicherstellt.

Bei schwerwiegenden Verstößen wesentlicher Einrichtungen kann die Cybersicherheitsbehörde darüber hinaus die zuständige Behörde ersuchen, Zertifizierungen oder Genehmigungen für die von der betroffenen Einrichtung erbrachten Dienste vorübergehend auszusetzen. Darüber hinaus besteht die Möglichkeit, Leitungsorganen einer wesentlichen Einrichtung zeitlich befristet die Wahrnehmung ihrer Leitungsaufgaben zu untersagen.

Das NISG 2026 betont ausdrücklich den Grundsatz der Verhältnismäßigkeit: Auswahl und Intensität der Durchsetzungsmaßnahmen müssen den Umständen des Einzelfalles Rechnung tragen. Maßgeblich sind insbesondere die Schwere und die Dauer des Verstoßes, etwaige einschlägige Vorverstöße, der verursachte Schaden sowie der Grad der Kooperation der Einrichtung mit der Cybersicherheitsbehörde.

6. Verhältnis zur DORA

6.1. Vorbemerkung

Für den Finanz- und Versicherungssektor ist das Verhältnis des NISG 2026 zur DORA von zentraler praktischer Bedeutung. Das NISG 2026 enthält in mehreren Bestimmungen klare Abgrenzungsregelungen, die den Vorrang der sektorspezifischen DORA-Regelungen ausdrücklich festschreiben und damit eine Doppelregulierung vermeiden sollen.

6.2. Grundsatz des Vorrangs der DORA

§ 4 Abs 2 NISG 2026 stellt klar, dass Angelegenheiten, die in den Anwendungsbereich der DORA fallen, vom NISG 2026 unbe-

rührt bleiben. Präzisiert wird dies in § 24 Abs 7 NISG 2026: Für Einrichtungen, die in den Anwendungsbereich der DORA fallen, kommen die einschlägigen Bestimmungen der DORA vorrangig zur Anwendung.

6.3. Versicherungsunternehmen: Anwendung der DORA statt des NISG 2026

Versicherungs- und Rückversicherungsunternehmen unterliegen – mit sogleich anzusprechenden Ausnahmen – grundsätzlich dem Anwendungsbereich der DORA und nicht dem NISG 2026. Diese Zuordnung ergibt sich aus dem Zusammenspiel mehrerer unions- und innerstaatlicher Rechtsgrundlagen:

Versicherungs- und Rückversicherungsunternehmen gelten gemäß Art 2 Abs 1 lit n iVm Abs 2 DORA als *„Finanzunternehmen"*, wodurch sie grundsätzlich in den Anwendungsbereich der DORA fallen. Dies gilt jedoch gemäß Art 2 Abs 3 lit b DORA nicht für jene Versicherungs- und Rückversicherungsunternehmen, die von Art 4 der Solvency II-Richtlinie[11] erfasst sind.[12]

In der Konsequenz haben die von der DORA erfassten Versicherungs- und Rückversicherungsunternehmen die Pflichten nach dem NISG 2026 nicht zu erfüllen. Dies betrifft insbesondere die Registrierungspflicht bei der Cybersicherheitsbehörde, die Abgabe einer Selbstdeklaration sowie die Meldung von Cybersicherheitsvorfällen an das nationale CSIRT. An ihre Stelle treten die spezifischen DORA-Anforderungen, die vergleichbare Regelungen enthalten.[13] Die Aufsicht über die Einhaltung dieser Anforderungen obliegt in Österreich der FMA und nicht der Cybersicherheitsbehörde. Verstöße gegen diese Anforderungen werden in Österreich mit Geldstrafen bis zu 150.000 € (für natürliche Personen bzw § 9 VStG-Verantwortliche) bzw (für juristische Personen) bis zu 500.000 € oder bis zu 1 % des jährlichen Gesamtnettoumsatzes[14] geahndet, je nachdem, welcher Betrag höher ist (§§ 7 und 8 DORA-VG).

Diese Abgrenzung stellt für von der DORA erfasste Versicherungs- und Rückversicherungsunternehmen eine wesentliche administrative Erleichterung dar, weil sie sich auf ein einheitliches regulatorisches Rahmenwerk konzentrieren können und keine parallelen Compliance-Strukturen für das NISG 2026 und die DORA aufbauen müssen. Gleichzeitig ist jedoch zu betonen, dass die DORA-Anforderungen in weiten Teilen strenger und detaillierter ausgestaltet sind als jene des NISG 2026. Die Befreiung vom NISG 2026 bedeutet daher nicht, dass die regulatorischen Anforderungen insgesamt weniger umfassend sind.

[11] Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. 11. 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II), ABl L 335 vom 17. 12. 2009, S 1.

[12] Die Richtlinie stellt hierfür auf bestimmte Merkmale ab.

[13] Vgl in diesem Zusammenhang etwa auch Delegierte Verordnung (EU) 2025/301 der Kommission vom 23. 10 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen, ABl L 2025/301 vom 20. 2. 2025, S 1; Durchführungsverordnung (EU) 2025/302 der Kommission vom 23. 10. 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung, ABl L 2025/302 vom 20. 2. 2025, S 1.

[14] Der Gesamtnettoumsatz bestimmt sich nach § 8 Abs 4 DORA-VG.

6.4. Besondere Stellung von IKT-Drittdienstleistern

Eine zentrale Klarstellung enthält § 24 Abs 8 NISG 2026, wonach IKT-Drittdienstleister im Sinne des Art 3 Z 23 DORA grundsätzlich auch den Bestimmungen des NISG 2026 unterliegen.

In der Praxis kann dies dazu führen, dass betroffene Dienstleister parallel beide Regelungsregime zu beachten haben. Maßgeblich sind dabei einerseits die DORA-Anforderungen für jene Leistungen, die gegenüber Finanzunternehmen erbracht werden, während für andere Tätigkeitsbereiche ergänzend oder alternativ die Pflichten nach dem NISG 2026 zur Anwendung gelangen.

Für Versicherungs- und Rückversicherungsunternehmen ist diese Regelung insbesondere bei der Auswahl, der vertraglichen Gestaltung und der laufenden Überwachung von IKT-Drittdienstleistern relevant. Sie müssen auch berücksichtigen, dass ihre Dienstleister unter Umständen sowohl den Anforderungen der DORA als auch jenen des NISG 2026 unterliegen. Die in der DORA vorgesehenen vertraglichen Mindestanforderungen an die Beziehung zu IKT-Drittdienstleistern (Art 28 Abs 3 und 4 DORA) bleiben davon unberührt und sind von erfassten Versicherungs- und Rückversicherungsunternehmen umzusetzen. Für die Vertragspraxis empfiehlt es sich, in Vereinbarungen mit IKT-Drittdienstleistern eine Klausel aufzunehmen, die den Dienstleister zur Einhaltung sowohl der DORA- als auch der NISG 2026-Anforderungen verpflichtet, soweit diese jeweils anwendbar sind. Ferner sollten Versicherungs- und Rückversicherungsunternehmen vertraglich sicherstellen, dass sie über wesentliche Cybersicherheitsvorfälle beim Dienstleister unverzüglich informiert werden, unabhängig davon, ob die Meldepflicht nach dem NISG 2026 oder der DORA ausgelöst wird.

7. Zwischenfazit

Das NISG 2026 markiert einen bedeutsamen Schritt in der Weiterentwicklung des österreichischen Cybersicherheitsrechts. Mit der Umsetzung der NIS-2-Richtlinie wird der Kreis der verpflichteten Einrichtungen erheblich ausgeweitet und es entsteht ein differenziertes System aus Pflichten, Aufsichtsmaßnahmen und Sanktionsinstrumenten. Die betroffenen Unternehmen und Organisationen stehen vor der Herausforderung, die erforderlichen Maßnahmen innerhalb der gesetzlich vorgegebenen Fristen umzusetzen und die Registrierungspflichten fristgerecht zu erfüllen.

Für die Versicherungsbranche ergibt sich ein differenziertes Bild: Versicherungs- und Rückversicherungsunternehmen fallen großteils als Finanzunternehmen primär unter die DORA und nicht unter das NISG 2026. Die maßgeblichen Anforderungen an Cybersicherheit, Risikomanagement und Vorfallmeldung ergeben sich für sie daher primär aus der DORA und den zugehörigen technischen Regulierungsstandards der europäischen Aufsichtsbehörden.[15]

IKT-Drittdienstleister, die Dienstleistungen für Versicherungs- und Rückversicherungsunternehmen erbringen, unterliegen hingegen beiden Regelungsregimen. Sie müssen die jeweils anwendbaren Anforderungen sorgfältig identifizieren und umsetzen.

[15] An dieser Stelle dürfen weitere Rechtsakte, aus denen sich gegebenenfalls einschlägige Pflichten ergeben, nicht vergessen werden, zB die DSGVO (Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung], ABl L 119 vom 4. 5. 2016, S 1).

8. Weitere produktbezogene und praxisrelevante Bedeutung

8.1. Vorbemerkung

Wenngleich das NISG 2026 selbst nicht in jedem Fall für das Versicherungs- oder Rückversicherungsunternehmen unmittelbar relevant ist,[16] kann es im Versicherungskontext dennoch erhebliche produktbezogene und damit praxisrelevante geschäftliche Bedeutung erlangen. Die Auswirkungen sind vielfältig und werden im Folgenden daher lediglich auszugsweise dargestellt.

8.2. Cyberrisikoversicherung und das NISG 2026

8.2.1. Einleitung

Neben der hier nicht weiter vertieften Bedeutung für individuelle Versicherungsverträge kommt dem NISG 2026 nach unserer Einschätzung insbesondere im Zusammenhang mit den vom Versicherungsverband Österreich (VVO) herausgegebenen Allgemeinen Bedingungen für die Cyberrisiko-Versicherung (ABC 2018)[17] zentrale Bedeutung zu (vorausgesetzt, das Gesetz ist im konkreten Fall anwendbar);[18] dies vor allem im Lichte der folgenden Themenkreise.

8.2.2. Risikoausschluss nach Art 2 ABC 2018

Art 2.7 ABC 2018 definiert einen Risikoausschluss für Situationen, in denen bestimmte genannte Personen vorsätzlich oder wissentlich insbesondere von Gesetzen, Verordnungen oder behördlichen Vorschriften abweichen und hierdurch ein Schaden, das heißt gegebenenfalls ein Versicherungsfall, entsteht. Ein vorsätzliches oder gar wissentliches schadenskausales Nichterfüllen der durch das NISG 2026 festgelegten Risikomanagementmaßnahmen (beispielsweise die Nichtumsetzung technisch gebotener Maßnahmen) oder ein diesbezügliches Fehlverhalten im Zusammenhang mit behördlichen Anordnungen könnte unserer Einschätzung nach unter diese Bestimmung fallen. Eine schadensursächliche Non-Compliance dieser Schwere stellt daher für den Versicherungsnehmer ein erhebliches Risiko dar, dass im Schadensfall aufgrund des Risikoausschlusses keine Versicherungsleistung erfolgt.

8.2.3. Obliegenheiten vor Eintritt des Versicherungsfalles

Art 9.1 ABC 2018, der die Obliegenheiten vor Eintritt des Versicherungsfalles regelt, bestimmt, dass *„alle für den versicherten Betrieb oder Beruf geltenden gesetzlichen und behördlichen Sicherheitsvorschriften … einzuhalten [sind].“*

Aufgrund des weitreichenden Anwendungsbereichs des NISG 2026 ist es nicht ausgeschlossen, auch dieses Gesetz unter die entsprechende Klausel zu subsumieren, wodurch es auch aus versicherungsvertraglicher Perspektive (insbesondere durch den Versicherungsnehmer) zu beachten sein wird. Andernfalls könnte eine Obliegenheitsverletzung vorliegen, die im Schadensfall – vorbehaltlich insbesondere der Bestimmungen des VersVG – möglicherweise zur Leistungsfreiheit des Versicherers führt.

Inwieweit unter Zugrundelegung dieses Verständnisses und aufgrund einer derartigen versicherungsvertraglichen Bezugnahme auf gesetzliche Regelungen (arg: *„gesetzlichen und behördlichen Sicherheitsvorschriften“* in Art 9.1 ABC 2018) wie etwa des NISG 2026 inhaltliche Redundanzen oder gar Widersprüche 1.) mit den übrigen Ziffern des Art 9 ABC 2018, 2.) mit explizit durch den Versicherer festgelegten und einzuhaltenden sonstigen Risikomanagementmaßnahmen, 3.) mit den restlichen Bedingungen oder 4.) sonstige interpretative Unklarheiten entstehen, ist eine im Einzelfall zu beurteilende Frage. Diese ist zudem dynamisch, weil sie sich an der fortlaufenden technischen Entwicklung orientiert (Stichwort: *„Stand der Technik“* gemäß § 32 Abs 2 NISG 2026).

Dementsprechend ist es empfehlenswert, Versicherungsbedingungen im Lichte der strengen Klauseljudikatur möglichst konkret und präzise zu gestalten, dynamische Verweise zu reduzieren sowie Redundanzen und Widersprüchlichkeiten zu bereinigen. So kann das latente Risiko einer möglichen Unwirksamkeit von Klauseln minimiert werden.

8.2.4. Obliegenheiten nach Eintritt des Versicherungsfalles

Ähnliche Überlegungen gelten im Zusammenhang mit Art 10 ABC 2018, der Obliegenheiten nach Eintritt des Versicherungsfalles vorsieht.

Eine gemäß § 34 NISG 2026 im Falle eines erheblichen Cybersicherheitsvorfalls gebotene Verständigung einschlägiger Stellen könnte bei extensiver Auslegung eine wesentliche Rolle im Kontext dieses Artikels spielen. So lässt sich etwa eine – zugegebenermaßen eher theoretische – Situation beschreiben, in der eine gebotene, jedoch im konkreten Schadensfall unterlassene oder verspätete Meldung zur Schadensabwendung oder -minderung (etwa durch eine frühere Unterstützung bei der Bewältigung des Vorfalls und Information betroffener Dritter) hätte beitragen können (§ 34 Abs 3, 4 und 6 NISG 2026). Bei Verstoß gegen eine solche Obliegenheit könnte – vorbehaltlich insbesondere der Bestimmungen des VersVG – ebenfalls Leistungsfreiheit des Versicherers eintreten.

8.3. Risikobewertung und Prämiengestaltung

Abseits etwaiger Obliegenheiten können die nach § 33 NISG 2026 erforderlichen Nachweise über die Umsetzung gebotener Risikomanagementmaßnahmen dazu beitragen, dass Versicherer bereits vor Versicherungsbeginn oder bei einer Verlängerung bzw einem *renewal* das individuelle Risiko eines (potenziellen) Versicherungsnehmers besser einschätzen und die Prämienhöhe entsprechend bemessen können.

8.4. Auswirkungen auf weitere Versicherungsprodukte

Die Relevanz des NISG 2026 sollte – auf Basis der vorstehenden Überlegungen – auch für verschiedene andere Versicherungsprodukte geprüft werden (insbesondere für Betriebsunterbrechungs-, Haftpflicht-, D&O- und Vertrauensschadensversicherungen).

Eine Berücksichtigung des NISG 2026 (insbesondere bei Neuabschlüssen oder *renewals*) sowie die Überprüfung bestehender Versicherungsverträge und gegebenenfalls die Konkretisierung oder Aktualisierung von Mustervertragswerken und Versicherungsbedingungen können im Lichte des neuen Gesetzes als sinnvoll angesehen werden.

8.5. Vertriebliche Aspekte

Selbst aus vertrieblicher oder marketingbezogener Perspektive bietet das NISG 2026 potenzielle Anknüpfungspunkte für Versicherer: Eine versicherungsmäßige Schadensabdeckung für das im Cyberumfeld häufig bestehende Restrisiko könnte beispielsweise als organisatorische Maßnahme gemäß § 32 NISG 2026 qualifiziert werden. Darüber hinaus kann eine entsprechende Versicherung – abhängig vom Produkt – auch zur Erfüllung technisch ge-

16 Siehe Punkt 7.

17 Online abrufbar unter https://vvonet.vvo.at/vvo/vvonet_website.nsf/sysPages/AB_Cyber.html/$file/Allgemeine_Bedingungen_fuer_die_CyberrisikoVersicherung_ABC_2018.pdf.

18 Gemeint ist damit, dass das NISG 2026 etwa auf den Versicherungsnehmer anwendbar ist; siehe auch https://www.schoenherr.eu/content/oesterreich-nisg-2026-alles-was-sie-wissen-mussen.

botener Risikomanagementmaßnahmen nach § 32 NISG 2026 beitragen (etwa durch die Bereitstellung von *Incident-response*-Leistungen im Rahmen des Versicherungsvertrages).

8.6. Bedeutung des Versicherungsschutzes aus NISG 2026-Sicht

Angesichts der vor allem im Cyberumfeld fehlenden Möglichkeit, sämtliche durch das NISG 2026 erfassten Risiken vollständig abzusichern, ist es aus unserer Sicht sinnvoll, dass die Geschäftsführung eines Unternehmens die Sinnhaftigkeit einer entsprechenden Versicherung evaluiert. Ein Abschluss ermöglicht oftmals den Transfer des verbleibenden Restrisikos, das selbst bei nach dem NISG 2026 hinreichend etablierten Risikomanagementmaßnahmen bestehen bleibt, auf den Versicherer.[19] Vor dem Hintergrund der erhöhten Sorgfaltsmaßstäbe für Vorstände und Geschäftsführer (etwa im Rahmen der Business Judgment Rule und der Governance-Verpflichtungen nach § 31 Abs 1 NISG 2026) erscheint ein dokumentiertes und nachvollziehbares Vorgehen, also die systematische Evaluierung und Entscheidungsdokumentation, als geradezu geboten.

Auf den Punkt gebracht

Das NISG 2026 setzt die europäische NIS 2-Richtlinie in österreichisches Recht um und erweitert den Kreis verpflichteter Einrichtungen erheblich, wobei insbesondere ein dreistufiges Pflichtenprogramm aus Governance-, Risikomanagement- und Meldepflichten eingeführt wird. Wesentliche und wichtige Einrichtungen müssen Risiken angemessen bewerten, Maßnahmen umsetzen, Nachweise erbringen, sich registrieren und erhebliche Cybersicherheitsvorfälle melden. Verstöße werden über ein abgestuftes Sanktionssystem und weitreichende Aufsichts- und Durchsetzungsbefugnisse der Cybersicherheitsbehörde geahndet. Für Versicherungs- und Rückversicherungsunternehmen gilt oftmals vorrangig die DORA; NISG 2026-Pflichten greifen meist nur subsidiär. IKT-Drittdienstleister können hingegen beiden Regimen unterliegen, was für Vertragsgestaltung, Überwachung und Compliance relevant ist.

Für Versicherer selbst bringt das NISG 2026 weitere wesentliche Neuerungen mit sich: Verstöße gegen das neue Gesetz können im Einzelfall zur Leistungsfreiheit führen, die gemäß § 33 NISG 2026 erforderlichen Nachweise über die Umsetzung gebotener Risikomanagementmaßnahmen lassen sich zudem für die interne Risikobewertung und die Prämiengestaltung nutzen und das NISG 2026 kann Auswirkungen auf verschiedene Versicherungsprodukte haben. Selbst für den Marketing- und Vertriebsbereich eröffnet das Gesetz Möglichkeiten; entsprechende Versicherungsprodukte könnten unter Umständen als organisatorische und/oder technische Risikomanagementmaßnahme qualifiziert werden.

[19] Weiterführend *A. Stadler/Drolz*, Pflicht und Kür bei der Abwehr von Cybercrime, Die Presse – Rechtspanorama vom 27. 2. 2023.

Bericht aus Brüssel

FiDA, der digitale Finanzmarktplatz

Dieter Pscheidl

Mag. Dieter Pscheidl ist Head of European Affairs bei der Vienna Insurance Group AG. Der vorliegende Beitrag gibt die persönliche Meinung des Autors wieder.

MEINUNG. *Dieter Pscheidl* ist seit 25 Jahren auf europäischer Ebene tätig. Im „Bericht aus Brüssel" teilt er seine Meinung zu aktuellen Diskussionen über europäische Versicherungspolitik und -regulierung.[1]

1. Einleitung

Stellen Sie sich vor, Sie loggen sich in Ihr Online-Banking ein und erhalten dort Alternativangebote externer Anbieter zu Ihren bestehenden Versicherungsverträgen. So ähnlich soll die neue Vertriebswelt nach FiDA aussehen. Die Abkürzung steht für Financial Data Access und bezeichnet einen Verordnungsvorschlag der Europäischen Kommission vom Juni 2023.[2] Das erklärte Leitmotiv von FiDA ist ein verbessertes Kundenangebot[3] durch mehr Wettbewerb, gepaart mit Innovation. Grundlage dafür wäre der Austausch von Kundendaten über eigens zu errichtende digitale Plattfor-

[1] Besonderer Dank gilt Mag. *Jeannine Weissel*, LL.M. für die wertvolle Unterstützung bei der Erstellung dieses Beitrags.

[2] KOM (2023) 360 endgültig, online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52023PC0360.

[3] Personenbezogene Bezeichnungen in diesem Beitrag beziehen sich immer auf alle Geschlechter. Aus Gründen der leichteren Lesbarkeit wird das generische Maskulinum verwendet.

Linde
Zeitschriften

Jetzt 20 % Rabatt auf Ihr Abo 2026!

Der perfekte Überblick
zum Versicherungsrecht

Praxis & Wissenschaft
Versicherungs- und Aufsichtsrecht

Rechtsprechung
OGH-Entscheidungen mit Glossen

Für die Praxis
RSS-Empfehlungen, Updates, News

shop.lindeverlag.at/zvers

Linde
Zeitschriften

ZVers – Jahresabonnement 2026

Bestellen unter:

- shop.lindeverlag.at/zvers
- fachzeitschriften@lindeverlag.at

Bitte geben Sie bei Ihrer Bestellung
den Aktionscode **V-26** an.

Print & Digital: **€ 255,90** (statt € 319,90)

Preisänderung und Irrtum vorbehalten.
(Preis inkl. MwSt., zzgl. Versandkosten)

Abbestellungen sind nur zum Ende eines Jahrganges möglich und müssen bis spätestens 30. November des Jahres schriftlich erfolgen. Unterbleibt die Abbestellung, so läuft das Abonnement automatisch auf ein Jahr und zu den jeweils gültigen Abopreisen weiter.

Weitere Informationen zur Zeitschrift
und alle Abo-Varianten finden Sie unter
shop.lindeverlag.at/zvers