

Erläuterungen

Allgemeiner Teil

Mit dem Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026), BGBl. I Nr. 94/2025, sollen in Umsetzung der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. L 333 vom 27.12.2022 S. 80, (im Folgenden: NIS-2-RL) Maßnahmen festgelegt werden, die ein hohes Cybersicherheitsniveau insbesondere wesentlicher und wichtiger Einrichtungen in den in § 2 NISG 2026 gelisteten Sektoren sicherstellen sollen. Mit dieser Verordnung der Cybersicherheitsbehörde werden zwei Regelungsbereichen näher bestimmt: Einerseits die Festlegung näherer Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit, andererseits weitere Kriterien über das Vorliegen eines erheblichen Cybersicherheitsvorfalls.

Zum ersten Regelungsbereich die näheren Anforderungen an die Risikomanagementmaßnahmen betreffend:

In Umsetzung des Art. 21 NIS-2-RL wird in § 32 NISG 2026 vorgesehen, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen haben. Diese Risikomanagementmaßnahmen sollen dazu dienen, die Sicherheit der Netz- und Informationssysteme, die für den Betrieb oder die Erbringung ihrer Dienste genutzt werden, zu gewährleisten sowie Cybersicherheitsvorfälle und deren Auswirkungen auf die Nutzer der jeweiligen Dienste und auf andere Dienste bestmöglich zu verhindern bzw. einzudämmen. Wesentlich ist, dass diese Risikomanagementmaßnahmen – nach der Systematik der NIS-2-RL – auf einem gefahrenübergreifenden Ansatz beruhen. Zudem sollen die Risikomanagementmaßnahmen ein dem bestehenden Risiko angemessenes Cybersicherheitsniveau zu gewährleisten haben, wobei der Stand der Technik, gegebenenfalls einschlägige nationale, europäische und internationale Normen sowie bewährte Verfahren und die von den betroffenen Einrichtungen zu tragenden Kosten berücksichtigt werden sollen. Demzufolge sollen die Risikomanagementmaßnahmen gewissen in § 32 Abs. 1 bis 4 NISG 2026 aufgezählten Mindestanforderungen entsprechen, wobei in § 32 Abs. 5 NISG 2026 vorgesehen ist, dass die Cybersicherheitsbehörde ermächtigt ist, mit Verordnung nähere Anforderungen an die Risikomanagementmaßnahmen gemäß Abs. 4 festzulegen.

Dabei sollen die von der Europäischen Kommission auf Grundlage des Art. 21 Abs. 5 NIS-2-RL erlassenen Durchführungsrechtsakte zur Festlegung technischer und methodischer Anforderungen an Risikomanagementmaßnahmen für bestimmte Sektoren – unter allfälliger Berücksichtigung sektorspezifischer Besonderheiten – auch auf andere Sektoren für anwendbar erklärt werden können, zumal diese Durchführungsrechtsakte allenfalls eine gute Basis auch für eine nähere Ausgestaltung der Risikomanagementmaßnahmen in anderen – grundsätzlich nicht erfassten – Sektoren darstellen.

Bei den Durchführungsrechtsakten auf Grundlage des Art. 21 Abs. 5 NIS-2-RL handelt es sich einerseits um solche, die die Europäische Kommission zum Zwecke der Festlegung der technischen und methodischen Anforderungen an die in Art. 21 Abs. 2 NIS-2-RL genannten Risikomanagementmaßnahmen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltzustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter verpflichtend zu erlassen hat. Andererseits ist sie darüber hinaus ermächtigt, (freiwillig) Durchführungsrechtsakte hinsichtlich der technischen und methodischen sowie erforderlichenfalls sektoralen Anforderungen an die in Art. 21 Abs. 2 NIS-2-RL genannten Maßnahmen auch in Bezug auf wesentliche und wichtige Einrichtungen, die in anderen Sektoren tätig sind, festzulegen.

Mit der Verordnung sollen auf Grundlage der Verordnungsermächtigung gemäß Art. 32 Abs. 5 NISG 2026 die gemäß Art. 2 samt Anhang der Durchführungsverordnung (EU) 2024/2690 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 Inhaltzustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer

Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, ABl. Nr. L 2024/2690 vom 18.10.2024, (im Folgenden DVO 2024/2690) festgelegten Anforderungen an die Risikomanagementmaßnahmen auf sämtliche in den Anlagen 1 und 2 des NISG 2026 gelisteten Arten von Einrichtungen erweitert werden, wodurch eine Konkretisierung der in § 32 Abs. 4 NISG 2026 festgelegten inhaltlichen Anforderungen an Risikomanagementmaßnahmen erfolgen und ausreichend Rechtssicherheit sowohl für die Behörde als auch die jeweiligen Einrichtungen geschaffen werden soll.

Durch den Verweis auf die DVO 2024/2690 in Bezug auf die Anforderungen an Risikomanagementmaßnahmen soll für sämtliche wesentlichen und wichtigen Einrichtungen des NISG 2026 ein einheitlicher Anforderungskatalog festgelegt werden und eine weitere Fragmentierung der Vorgaben vermieden werden. Dieser Anforderungskatalog soll zwar als umfassender Rahmen, in dem sich die wesentlichen und wichtigen Einrichtungen bewegen sollen, dienen, er stellt jedoch keine konkrete Umsetzungsbeschreibung von Maßnahmen für die jeweiligen Einrichtungen dar. Hinsichtlich der konkreten Umsetzung von Risikomanagementmaßnahmen anhand des Anforderungskatalogs durch eine Einrichtung besteht ein gewisser Umsetzungsspielraum im Sinne eines „risikobasierten Ansatzes“ (insb. verhältnismäßig, dem bestehenden Risiko angemessen), welcher durch § 32 Abs. 1 bis 4 NISG 2026 vorgegeben wird.

Zum zweiten Regelungsbereich weitere Kriterien über das Vorliegen eines erheblichen Cybersicherheitsvorfalls betreffend:

In diesem Regelungsbereich sollen aufgrund des § 35 Abs. 3 NISG 2026 nähere Kriterien festgelegt werden, nach denen ein Cybersicherheitsvorfall als erheblich einzustufen ist.

Die Cybersicherheitsbehörde kann gemäß § 35 Abs. 3 NISG 2026 mit Verordnung weitere Kriterien und nähere Regelungen zu Abs. 2 für das Vorliegen eines erheblichen Cybersicherheitsvorfalls festlegen. Dabei können sektorspezifische Faktoren berücksichtigt werden. Diese Spezifizierung sektorspezifischer Faktoren durch Verordnung wird sich an den jeweiligen aktuellen tatsächlichen Gegebenheiten orientieren. Dies kann unter anderem auch eine Änderung der Rechtsansichten der Mitgliedstaaten über die Erheblichkeit von Sicherheitsvorfällen (für bestimmte Sektoren) umfassen.

In diesem Regelungsbereich soll Art. 23 Abs. 3 NIS-2-Richtlinie im Vollzug umgesetzt und näher festgelegt werden, wann ein Cybersicherheitsvorfall jedenfalls als nach § 34 NISG 2026 meldepflichtiger „erheblicher Cybersicherheitsvorfall“ einzustufen ist.

Gemäß § 35 Abs. 1 NISG 2026 gilt ein Cybersicherheitsvorfall als erheblich, wenn dieser schwerwiegende Betriebsstörungen der erbrachten Dienste der Einrichtung oder schwerwiegende finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Angesichts der zentralen Rolle der Durchführungsverordnung (EU) 2024/2690 der Europäischen Kommission vom 17. Oktober 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 Inhaltzustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, orientiert sich diese Verordnung an die Systematik und Kernaspekte der Durchführungsverordnung (EU) 2024/2690.

Nicht-sektorspezifische Kriterien und die Struktur der DVO 2024/2690 sind geeignet, nationalstaatlich sektorübergreifend angewendet zu werden. Eine möglichst weitgehende Anlehnung reduziert den Aufwand für Adressaten (insbesondere bei Anwendbarkeit mehrerer Normen) und trägt zu einer weiteren Harmonisierung bei. Erwägungsgründe der DVO 2024/2690 sollen dementsprechend bei der Anwendung dieser Verordnung mitzubерücksichtigen sein.

Darüber hinaus sind die in § 35 Abs. 2 NISG 2026 genannten und bei der Beurteilung der Erheblichkeit ebenfalls zu berücksichtigenden Kriterien jenen Kriterien nachempfunden, die bereits für die Beurteilung eines „Sicherheitsvorfalls“ nach dem NISG idF BGBl. I Nr. 111/2018 (§ 3 Z 6 NISG) zu berücksichtigen waren. Insbesondere unternehmens- und sektorspezifische Faktoren nach § 35 Abs. 2 Z 6 NISG 2026 (z.B. sektorspezifische Vorschriften) sind bei der Beurteilung sektorspezifischer Sachverhalte weiterhin zu berücksichtigen.

Bestimmungen der DVO 2024/2690 sowie die Geltung dieser für Einrichtungen, die der DVO 2024/2690 unterliegen, bleiben durch die in dieser Verordnung festgelegten Kriterien unberührt.

Ebenso bleiben sonstige Vorschriften, aus denen sich eine Meldepflicht ergibt unberührt. Unberührt bleiben insbesondere Bestimmungen der Verordnung des Bundesministers für Inneres zur Durchführung des Resilienz kritischer Einrichtungen-Gesetzes Resilienz kritischer Einrichtungen-Verordnung – RKEV), BGBl. II Nr.91/2026 sowie § 123 Abs. 4 TKG 2021, wonach in § 123 Abs. 1 TKG 2021 genannte Anbieter und Betreiber der Regulierungsbehörde, den betroffenen Bescheidinhabern von Notrufnummern sowie den betroffenen Notrufabfragestellen Sicherheitsvorfälle, die beträchtliche Auswirkungen auf die Erreichbarkeit von Notrufnummern hatten, unverzüglich mitzuteilen haben.

Besonderer Teil

Zu § 1 (Gegenstand):

Mit dieser Verordnung sollen nähere Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sowie weitere Kriterien für das Vorliegen eines erheblichen Cybersicherheitsvorfalls festgelegt werden.

Zu § 2 (Anforderungen an Risikomanagementmaßnahmen):

Mit der auf Grundlage des Art. 21 Abs. 5 NIS-2-RL erlassenen unmittelbar geltenden DVO 2024/2690, in die auch Überlegungen bzw. Ergebnisse einer spezifischen Arbeitsgruppe im Rahmen der Cyber Sicherheit Plattform (CSP) betreffend Risikomanagementmaßnahmen im 1. Halbjahr 2024 unter Einbindung betroffener Stakeholder eingeflossen sind, werden gemäß Art. 2 in Verbindung mit dem Anhang die technischen und methodischen Anforderungen an die in Art. 21 Abs. 2 lit. a bis j NIS-2-RL genannten Risikomanagementmaßnahmen 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 festgelegt.

Die in der DVO 2024/2690 festgelegten Anforderungen an Risikomanagementmaßnahmen sind zwar unmittelbar lediglich für bestimmte Arten von Einrichtungen anzuwenden, aufgrund ihrer allgemeinen Formulierung stellen sie jedoch auch für nicht umfasste Arten von Einrichtungen grundsätzlich geeignete und verhältnismäßige Anforderungen an Risikomanagementmaßnahmen dar, weshalb vor dem Hintergrund der Konsistenz, Vereinheitlichung und Vereinfachung eine entsprechende Ausdehnung ihres Anwendungsbereichs erfolgen soll.

Durch diese Vorgehensweise soll zudem verhindert werden, dass betroffene Einrichtungen unterschiedlichen Anforderungen bzw. Vorgaben unterliegen, wodurch – auch in Anbetracht allfälliger zukünftiger Entwicklungen auf Unionsebene – eine bessere Planbarkeit und zielgerichtete Umsetzung für die jeweiligen Einrichtungen ermöglicht werden soll. Die Erwägungsgründe der DVO 2024/2690, welche die technischen und methodischen Anforderungen an Risikomanagementmaßnahmen im Bereich der Cybersicherheit betreffen (siehe ErwGr 3 bis 29) sollen auch im Rahmen dieser Verordnung als Erläuterung und Auslegungshilfe dienen (bspw. wird in ErwGr 10 festgehalten, dass der Begriff „Nutzer“ alle juristischen und natürlichen Personen erfassen sollte, die Zugang zu den Netz- und Informationssystemen der Einrichtung haben).

Zudem sollen im Sinne eines kohärenten Systems die öffentlich verfügbaren Unterlagen der ENISA (insb. „ENISA Technical Implementation Guidance“ und „ENISA Technical Implementation Guidance Mapping Table“, abrufbar unter <https://www.enisa.europa.eu>) sowie auch der NIS-Kooperationsgruppe („Referenzdokument zu Sicherheitsmaßnahmen für Einrichtungen im Rahmen der NIS2“ und „Anhang Referenzdokument zu Sicherheitsmaßnahmen für Einrichtungen im Rahmen der NIS2 – Zuordnungstabelle“, abrufbar unter <http://digital-strategy.ec.europa.eu>) als Leitfäden und technische Erläuterungen fungieren.

In Punkt 3.4.2 lit. b im Anhang der DVO 2024/2690 wird im Zusammenhang mit der Bewertung und Klassifizierung von Ereignissen auf Art. 4 der DVO 2024/2690 verwiesen. § 7 der gegenständlichen Verordnung soll systematisch an Art. 4 anknüpfen, weshalb jene Einrichtungen, die nicht ohnehin von der DVO 2024/2690 unmittelbar betroffen sind, § 7 analog zu Art. 4 heranziehen sollen. Wesentlich ist, dass die Regelungen bezüglich der Anforderungen gemäß § 32 NISG 2026 und demnach auch jene gemäß der auf Basis dieser Rechtsgrundlage zu erlassenden Verordnung insoweit nicht anwendbar sein sollen, als wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer unionsrechtlicher Bestimmungen zur Ergreifung von Risikomanagementmaßnahmen verpflichtet sind, sofern diese ein zumindest gleichwertiges Cybersicherheitsniveau gewährleisten (vgl. § 27 NISG 2026 sowie Art. 4 NIS-2-RL). In diesem Zusammenhang ordnet etwa die unmittelbar anwendbare Regelung gemäß Art. 1 Abs. 2 der Verordnung (EU) 2022/2554 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) Nr. 2016/1011, ABl. Nr. L 333 vom 27.12.2022 S. 1, (im Folgenden: DORA-VO) ausdrücklich an, dass die DORA-VO für Finanzunternehmen, die als wesentliche oder wichtige Einrichtungen gelten, als sektorspezifischer Rechtsakt gemäß Art. 4 NIS-2-RL gilt.

Zu § 3 (Risikokategorien):

Diese Bestimmung soll festlegen, dass sich wesentliche und wichtige Einrichtungen nach dem NISG 2026 an den generisch gehaltenen Rahmen von zumindest vier übergeordneten Risikokategorien zu orientieren und diesen bei ihrem Risikomanagementverfahren im Bereich der Cybersicherheit zu berücksichtigen haben (siehe dazu Anhang der DVO – 2. Konzept für das Risikomanagement – 2.1 Risikomanagementrahmen). Es soll damit insb. Einrichtungen helfen, die noch über kein fundiertes Risikomanagementverfahren verfügen.

Die Einführung dieser Risikokategorien soll nicht dazu führen, dass betroffene Einrichtungen bestehende Risikomanagementsysteme systemisch umbauen müssen, der qualitative Grad der Risikokategorien ist nämlich so gewählt, dass eine von jeweils bestehenden und zu identifizierenden Risiken über sämtliche Sektoren hinweg und zu mehreren Risikokategorien möglich erscheint. Es soll demnach möglich sein, dass von den Einrichtungen identifizierte Risiken mehreren dieser Risikokategorien und über diese hinaus zugeordnet werden können.

Es soll dadurch auch eine Informationsbasis für die Cybersicherheitsbehörde geschaffen werden, um einen risikobasierten Vollzug ausgestalten sowie Meta-Risikoanalysen innerhalb eines Sektors oder sektorübergreifend durchführen zu können.

Die Risikokategorie „Technologische Risiken“ (Z 1) soll mögliche Risiken betreffen, die sich aus Gefahren im Zusammenhang mit dem Umgang und Einsatz von Technologien (z.B. Cloud, Virtualisierungen, Künstlicher Intelligenz etc.) aus systemischer bzw. strategischer Sicht sowie operativer Sicht in Bezug auf die Netz- und Informationssysteme der jeweiligen wesentlichen oder wichtigen Einrichtung ergeben können.

Die Risikokategorie „Menschliche Risiken“ (Z 2) soll mögliche Risiken betreffen, die sich aus Gefahren im Zusammenhang mit dem „menschlichen“ Verhalten („Human Factor“) des Personals der jeweiligen wesentlichen oder wichtigen Einrichtung in Bezug auf intentionales (z.B. Insider Threat) und unintentionales Verhalten (z.B. unbewusste Fehlkonfiguration) ergeben können. Hierzu sollen auch mögliche Risiken gezählt werden, die sich aus Gefahren im Zusammenhang mit der Ausnutzung menschlicher Schwächen durch Einflussnahme auf das Personal der jeweiligen Einrichtung (z.B. Social Engineering) aber auch im Zusammenhang mit psychologischen Faktoren das Personal betreffend wie bspw. Stress und Zeitdruck, Belastungszustände, Gewohnheiten, Vertrauen etc. (z.B. auch bei Entscheidungen oder Prozessabläufen) ergeben können.

Die Risikokategorie „Risiken in der IKT-Lieferkette“ (Z 3) soll sich auf mögliche Risiken beziehen, die sich aus Gefahren im expliziten Zusammenhang mit der IKT-Lieferkette der jeweiligen wesentlichen oder wichtigen Einrichtung (z.B. die Abhängigkeit von einem bestimmten Dienstleister) ergeben können.

Die Risikokategorie „Standortbezogene Risiken für Netz- und Informationssystemen“ (Z 4) soll mögliche Risiken betreffen, die sich aus physischen Gefahren in Bezug auf die Netz- und Informationssysteme am jeweiligen Standort der wesentlichen oder wichtigen Einrichtung (z.B. Naturkatastrophen wie Hochwasser, Brände, aber auch z.B. unbefugter Zutritt von Personen) ergeben können.

Zu § 4 (Kompensierende Maßnahmen):

Mit dieser Bestimmung soll an den Inhalt des ErwGr 5 der DVO 2024/2690 angeknüpft werden, welcher besagt, dass Einrichtungen die Möglichkeit haben sollten, Ausgleichsmaßnahmen zu treffen, wenn die Umsetzung der technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit aus bestimmten Gründen nicht möglich ist.

Anstatt des Begriffes „Ausgleichsmaßnahme“ soll hier der treffendere Begriff „kompensierende Maßnahme“ verwendet werden, da dieser in praxi gebräuchlicher ist und dem in der englischen Fassung der DVO 2024/2690 verwendeten Begriff „compensating measures“ entspricht. In Abs. 1 sollen die beiden Fälle definiert werden, in denen statt der Pflicht zur Entsprechung einer jeweiligen Anforderung gemäß § 2 lediglich die Verpflichtung zur Umsetzung kompensierender Maßnahmen besteht:

Fall 1 – Anforderungen kann aufgrund der Größe nicht entsprochen werden:

Mit der Größe einer Einrichtung soll im Grunde an die Größenkategorien von Unternehmen (Kleinstunternehmen, kleine Unternehmen, mittlere Unternehmen und große Unternehmen) angeknüpft werden. Hierbei sollen die Mitarbeiteranzahl sowie Jahresumsatz bzw. Jahresbilanzsumme im Sinne von

§ 25 NISG 2026 angesetzt werden. Zudem kann auch eine bestehende organisatorische Komplexität (z.B. durch mehrere Standorte) miteinbezogen werden.

Kleinere Unternehmen haben in Bezug auf die Umsetzung von entsprechenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit in der Regel geringere finanzielle und personelle Ressourcen, weniger spezifisches Fachwissen und dadurch begrenztere Umsetzungskapazitäten. Dieser mögliche Umstand soll hier Berücksichtigung finden.

Die hier verwendete Anknüpfung an die Größe einer Einrichtung soll jedoch nicht dazu führen, dass der jeweilige individuelle Schutzbedarf einer Einrichtung von der Unternehmensgröße bzw. Größe der Einrichtung abgeleitet wird und als pauschales Argument verwendet wird, um die Pflicht zur regulären Entsprechung der Anforderungen an Risikomanagementmaßnahmen zu umgehen.

Fall 2 – Anforderungen kann vorübergehend nicht entsprochen werden:

Beim zweiten Fall handelt es sich um Konstellationen, bei denen es in der Natur der Sache liegt, dass zur Entsprechung einer Anforderung gemäß § 2 bestimmte Umstände die Umsetzung zum aktuellen Zeitpunkt verhindern – etwa einzuhaltende Fristen eines Vergabeverfahrens zur Beschaffung von zur Entsprechung der Anforderungen nötigen Produkten oder Dienstleistungen oder längerfristige Umsetzungsprojekte (z.B. Tausch eines Leitsystems). Der jeweiligen Anforderung ist in diesem Fall somit lediglich zeitlich begrenzt nicht verpflichtend zu entsprechen.

In Abs. 2 soll genauer definiert werden, welche Voraussetzungen kompensierende Maßnahmen zu erfüllen haben: Durch ihre Umsetzung ist dem Zweck einzelner Anforderungen, denen jeweils momentan oder aufgrund der Größe einer Einrichtung nicht entsprochen werden kann und der Minimierung des oder der mit der dahinterliegenden Risikomanagementmaßnahme behandelten Risikos oder Risiken so gut wie möglich zu dienen. Der Zweck der jeweiligen Anforderung sollte sich aus der jeweiligen Anforderung bzw. Teilanforderung selbst oder dem jeweils übergeordneten Kapitel zur Anforderung ergeben. Der Anspruch an kompensierende Maßnahmen soll aber eben nicht der gleiche sein, wie an die Anforderungen gemäß § 2. Es soll hier zugestanden werden, dass in Fällen, in denen eine Entsprechung der Anforderungen des § 2 (temporär) nicht möglich ist, stattdessen Maßnahmen zu treffen sein sollen, mithilfe derer trotzdem noch ein möglichst hohes Schutzniveau erreicht wird. Außerhalb der beiden oben beschriebenen Fälle sollen kompensierende Maßnahmen somit nicht den Anforderungen des § 2 genügen.

Die Minimierung der verbundenen Risiken soll auf Basis einer durchgeführten Risikobewertung erfolgen. Dies soll insb. verdeutlichen, dass es einrichtungsseitig einer entsprechenden internen Auseinandersetzung mit den durch die Nichtumsetzung der ursprünglichen Risikomanagementmaßnahme entstandenen und damit verbundenen Risiken bedarf. Dieser durchgeführte Prozess sowie die daraus resultierenden Ergebnisse sind entsprechend zu dokumentieren (siehe Abs. 3).

Mit Abs. 3 soll geregelt werden, dass kompensierende Maßnahmen stets nachvollziehbar und begründet zu dokumentieren und regelmäßig, zumindest jährlich, auf deren Wirksamkeit hin zu überprüfen sind. Als Maßstab für die Überprüfung der Wirksamkeit sollen die generellen Anforderungen nach Abs. 2 herangezogen werden. Damit soll auch der Cybersicherheitsbehörde ermöglicht werden, zu prüfen, ob diese den Vorgaben entsprechen.

In Abs. 4 soll klargestellt werden, dass die Umsetzung von kompensierenden Maßnahmen durch wesentliche oder wichtige Einrichtungen unter bestimmten Umständen unterbleiben kann. Vom Verweis auf Art. 2 der DVO 2024/2690 in § 2 ist nämlich auch Art. 2 Abs. 2 UAbs. 2 umfasst, welcher im Sinne eines „Comply or Explain“-Ansatzes Folgendes regelt: Ist im Anhang der DVO 2024/2690 vorgesehen, dass einer technischen oder methodischen Anforderung einer Risikomanagementmaßnahme im Bereich der Cybersicherheit nur zu entsprechen ist, soweit dies angemessen, anwendbar oder durchführbar ist, und hält es die betreffende Einrichtung für nicht angemessen, nicht anwendbar oder nicht durchführbar, bestimmten Anforderungen zu entsprechen, so muss die betreffende Einrichtung ihre diesbezügliche Begründung in verständlicher Weise dokumentieren.

In Bezug auf jene ausdrücklich im Anhang der DVO 2024/2690 genannten Fälle von Teilanforderungen oder Anforderungen an Risikomanagementmaßnahmen (z.B. Teilanforderung in 1.1.2 [... und – soweit angemessen – aktualisiert. ...], Anforderung in 1.2.5 [... werden – soweit anwendbar – getrennt.], Teilanforderung in 3.2.2 [...Soweit durchführbar...]) soll es für sämtliche wesentlichen und wichtigen Einrichtungen ausreichen, die Nichtumsetzung lediglich begründet zu dokumentieren.

Zu § 5 (Erhebliche Cybersicherheitsvorfälle)

§ 5 legt für Einrichtungen, die einem Sektor außerhalb des Geltungsbereichs der Durchführungsverordnung (EU) 2024/2690 zuzuordnen sind, fest, wann Erheblichkeit im Sinne des § 35 Abs. 1 NISG 2026 vorliegt. Das Vorliegen eines erheblichen Cybersicherheitsvorfalls löst Melde- und Berichtspflichten nach § 34 NISG 2026 aus. Die Erheblichkeit muss sich dabei auf einen konkreten

Cybersicherheitsvorfall im Sinne des § 3 Z 30 NISG 2026 beziehen. Ein Cybersicherheitsvorfall ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt. Berichtspflichten nach § 34 NISG 2026 können bei Vorliegen der entsprechenden Vertretungsbefugnis auch durch Dritte im Namen einer § 34 Abs. 1 NISG 2026 unterliegenden Einrichtung erfüllt werden. Im Zuge der Aktualisierung von Informationen (§ 34 Abs. 2 Z 2 NISG 2026) haben Einrichtungen bei Nichtvorliegen der Voraussetzungen nach § 35 NISG 2026 gegebenenfalls einen Widerruf der Meldung kundzutun.

§ 5 Abs. 1 Z 1 bis 6 erfolgen in Anlehnung an Art. 3 der Durchführungsverordnung (EU) 2024/2690, wobei die Möglichkeit zur Verursachung in Z 1 bis Z 3 dann gegeben ist, wenn damit zu rechnen ist, dass die jeweilige Auswirkung bei gewöhnlichem Verlauf der Dinge in naher Zukunft eintreten wird, somit kurz bevorsteht.

§ 5 Abs. 1 Z 1 entspricht Art. 3 Abs. 1 lit. a der Durchführungsverordnung (EU) 2024/2690, wobei auf den jährlichen Gesamtumsatz, aufgrund dessen die Einrichtung in den Anwendungsbereich fällt, abzustellen ist. (siehe § 25 Abs. 1 NISG 2026 unter Anwendung der Art. 1 bis 6 des Anhangs der Empfehlung 2003/361/EG der Kommission vom 06. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. Nr. L 124 vom 20.5.2003 S. 36, mit Ausnahme des Art. 3 Abs. 4 des Anhangs dieser Empfehlung).

Bei der Bestimmung der direkten finanziellen Verluste infolge eines Cybersicherheitsvorfalls sollten die betreffenden Einrichtungen alle finanziellen Verluste berücksichtigen, die ihnen infolge des Cybersicherheitsvorfalls entstanden sind, wie etwa Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur, Personalkosten, einschließlich Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung zusätzlichen Personals, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen, Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen, Kosten für Ausgleichs- und Entschädigungszahlungen an Kunden, Verluste wegen entgangener Einnahmen, Kosten für interne und externe Kommunikation, Beratungskosten, einschließlich Kosten im Zusammenhang mit Rechtsberatung, forensischen Dienstleistungen und Behebungsdienstleistungen, und sonstige Kosten im Zusammenhang mit dem Cybersicherheitsvorfall. Geldbußen wie auch Kosten, die für den laufenden Geschäftsbetrieb erforderlich sind, sollten jedoch nicht als finanzielle Verluste infolge eines Sicherheitsvorfalls betrachtet werden, darunter etwa Kosten für die allgemeine Wartung von Infrastruktur, Ausrüstung, Hardware und Software, Kosten für die laufende Fortbildung des Personals, um dessen Kompetenzen auf dem aktuellen Stand zu halten, interne oder externe Kosten für die Verstärkung des Geschäftsbetriebs nach dem Vorfall, einschließlich für Aufrüstungen, Verbesserungen und Initiativen zur Risikobewertung, sowie Versicherungsprämien. Die betreffenden Einrichtungen sollten die Höhe der finanziellen Verluste auf der Grundlage vorliegender Daten berechnen; wenn die tatsächliche Höhe der finanziellen Verluste nicht bestimmt werden kann, sollten die Einrichtungen solche Beträge schätzen.

§ 5 Abs. 1 Z 2 entspricht Art 3 Abs. 1 lit. b der Durchführungsverordnung (EU) 2024/2690, wobei durch das Anknüpfen an den Abfluss von Geschäftsgeheimnissen bzw. geheime Informationen durch den Verweis auf das UWG bzw. das IFG auf die nationale Rechtslage Rücksicht genommen werden soll. Mitumfasst sind dadurch insbesondere auch Informationen im Bereich der Einrichtungen der öffentlichen Verwaltung und im Bereich des geistigen Eigentums.

Zudem soll durch das Abstellen auf die Wahrscheinlichkeit in § 5 Abs. 1 Z 5 nicht bloß die Geeignetheit, schwerwiegende Betriebsstörungen zu verursachen, ausreichen, sondern soll darüber hinaus diese Folge wahrscheinlich sein. Dies ist dann der Fall, wenn aus der Sicht eines objektiven Dritten und bei gewöhnlichem Verlauf der Dinge, aufgrund der bekannten tatsächlichen Umstände mehr Gründe für den Eintritt einer schwerwiegenden Betriebsstörung sprechen als für den Nichteintritt.

Ein erheblicher Cybersicherheitsvorfall liegt auch dann vor, wenn der Cybersicherheitsvorfall zum Ausfall oder zur eingeschränkten Verfügbarkeit für die Nutzer der von der Einrichtung erbrachten Dienste im Gebiet zumindest eines Bundeslandes für mehr als 24 Stunden geführt hat oder dazu führen kann. Dadurch werden erhebliche Cybersicherheitsvorfälle in ihrer geografischen Ausbreitung erfasst. Abgestellt wird nicht auf die territoriale Fläche, sondern auf die Nutzeranzahl im jeweiligen Bundesland, soweit eine territoriale Zuordenbarkeit faktisch möglich ist. Nutzer sind dabei insbesondere diejenigen, die Dienste einer Einrichtung tatsächlich in Anspruch nehmen oder deren Inanspruchnahme konkret geplant oder eingeleitet ist (z.B. bei Einrichtungen des Gesundheitswesens ebenfalls Personen, die während des Cybersicherheitsvorfalls zur Inanspruchnahme des betroffenen Dienstes aufgenommen oder angemeldet werden). Eine bloß abstrakte Möglichkeit, die Dienste einer Einrichtung künftig in Anspruch zu nehmen reicht jedoch nicht aus. Eine eingeschränkte Verfügbarkeit liegt insbesondere dann vor, wenn

wenn ein von einer betreffenden Einrichtung erbrachter Dienst deutlich langsamer ist, als die durchschnittliche Reaktionszeit oder wenn nicht alle Funktionen eines Dienstes verfügbar sind.

Die von der Einrichtung erbrachten Dienste im Sinne dieser Verordnung sind jene Dienste, aufgrund derer die Einrichtung in den Anwendungsbereich fällt (Einrichtungen der in den Anlagen 1 und 2 NISG 2026 genannten Art).

Zudem liegt ein erheblicher Cybersicherheitsvorfall auch dann vor, wenn er zur Aktivierung des Krisenmanagements oder von Notfallwiederherstellungsplänen des Betriebskontinuitätsmanagements geführt hat. Dies ist in Zusammenhang mit den Anforderungen zum Krisenmanagement im Bereich der Risikomanagementmaßnahmen zu sehen. Einrichtungen sind im Zuge der Umsetzung von Risikomanagementmaßnahmen dazu verpflichtet, Maßnahmen im Kontext des Krisenmanagements bzw. des Betriebskontinuitätsmanagement zu setzen. Diese haben angemessen und wirksam zu sein. Die Aktivierung des Krisenmanagements zum gebotenen Zeitpunkt, insbesondere bei Erreichen der einschlägigen internen Eskalationsstufen indiziert Erheblichkeit im Sinne des § 35 Abs. 1 NISG 2026.

Zu § 6 (Planmäßige Betriebsunterbrechungen)

Planmäßige Betriebsunterbrechungen und geplante Folgen planmäßiger Wartungsarbeiten im Sinne des § 6 sollen nicht zur Einstufung einer Erheblichkeit führen. Nicht planmäßige Unterbrechungen und ungeplante Folgen sind bereits begrifflich nicht von § 6 erfasst und sind nach den übrigen Bestimmungen zu beurteilen. Bei Zeiträumen außerhalb der vertraglich bedungenen Leistungszeiten, scheitert es in der Regel an der Betroffenheit Dritter.

Zu § 7 (Wiederholte Cybersicherheitsvorfälle)

In § 7 wird klargestellt, dass Cybersicherheitsvorfälle, die einzeln betrachtet nicht als erhebliche Cybersicherheitsvorfälle anzusehen sind, zusammengenommen als ein erheblicher Cybersicherheitsvorfall gelten, wenn alle in § 7 genannten Kriterien kumulativ erfüllt sind. Es handelt sich dabei um eine Anlehnung an Art. 4 der Durchführungsverordnung (EU) 2024/2690 (Wiederholte Sicherheitsvorfälle); in Bezug auf den Verweis auf Art. 4 in Punkt 3.4.2 lit. b im Anhang der DVO 2024/2690 (vgl. Erläuterungen zu § 2).

Wiederholte Cybersicherheitsvorfälle können auf erhebliche Mängel und Schwächen in den Verfahren für das Cybersicherheitsrisikomanagement der betreffenden Einrichtung und deren Reifegrad im Bereich der Cybersicherheit hindeuten. Darüber hinaus können solche wiederholten Cybersicherheitsvorfälle erhebliche finanzielle Verluste bei der betreffenden Einrichtung verursachen.

§ 7 Z 2 knüpft dabei neben der Ursache zusätzlich an die Auswirkung des Cybersicherheitsvorfalls an, die bei den zu betrachtenden Cybersicherheitsvorfällen für eine Anwendung des § 7 ebenfalls der Art nach dieselbe sein muss. Neben dem Bedrohungsfeld wird somit zusätzlich auch das Bedrohungsziel angeknüpft und der wiederholte Cybersicherheitsvorfall näher konkretisiert. Ein wiederholter Cybersicherheitsvorfall nach § 7 kann demnach insbesondere dann vorliegen, wenn Hinweise dafür vorliegen, dass es sich um denselben Bedrohungsakteur handelt, die gleiche Vorgehensweise vorliegt, es sich um denselben Angriffsvektor handelt, der Cybersicherheitsvorfall sich auf den gleichen Zeitpunkt bezieht, ein gleichartiges betroffenes Gut vom Cybersicherheitsvorfall betroffen ist oder das gleiche Angriffsziel gegeben ist.

Zu § 8 (Verweisungen):

Verweisungen auf andere Bundesgesetze sind grundsätzlich als Verweisungen auf die jeweils geltende Fassung zu verstehen. Demgegenüber sind Verweisungen, die auf ein Gesetz in einer bestimmten Fassung verweisen, nicht als Verweisungen auf die jeweils geltende Fassung zu verstehen. Verweisungen auf europäische Rechtsakte sind darüber hinaus als Verweisungen auf die zum Zeitpunkt des Inkrafttretens geltende Fassung zu verstehen, sofern die entsprechende Bestimmung nicht ohnehin zur besseren Verständlichkeit direkt in die Verordnung übernommen wurde.

Zu § 9 (Inkrafttreten):

Diese Bestimmung soll das Inkrafttreten regeln.