

An das
Bundesministerium für Inneres
Herrengasse 7
1010 Wien

Wien, am 24.08.2026

Stellungnahme der ISPA zum Entwurf der Risikomanagementmaßnahmen-Verordnung (RMMV) sowie der Verordnung über die Erheblichkeit von Cybersicherheitsvorfällen (ECV) gemäß NISG 2026

Sehr geehrte Damen und Herren!

Die ISPA - Internet Service Providers Austria - bedankt sich für die Möglichkeit zur Stellungnahme zu den Entwürfen der Risikomanagementmaßnahmen-Verordnung (RMMV) sowie der Verordnung über die Erheblichkeit von Cybersicherheitsvorfällen (ECV) und nimmt dazu wie folgt Stellung. Die grundsätzliche Orientierung der Entwürfe an der Durchführungsverordnung (EU) 2024/2690 (DVO) wird begrüßt, da dies zu einem einheitlichen, sektorübergreifenden Rahmen beiträgt. In mehreren Punkten gehen die Entwürfe jedoch über die DVO hinaus bzw. weichen von deren Systematik ab, wodurch aus Sicht der ISPA und ihrer Mitglieder Klarstellungen bzw. Anpassungen erforderlich erscheinen.

I. Zur Risikomanagementmaßnahmen-Verordnung (RMMV)

1. Verpflichtende Risikokategorien

Der Entwurf sieht vor, dass im Rahmen der Risikoanalyse zumindest vier Risikokategorien – technologische Risiken, menschliche Risiken, Risiken in der IKT-Lieferkette sowie standortbezogene Umweltrisiken – zu verwenden sind. Diese Vorgabe geht über die DVO hinaus, die im Anhang lediglich die Einrichtung eines „Risikomanagementrahmens“ fordert, ohne konkrete Risikokategorien verbindlich festzulegen. Problematisch ist insbesondere, dass die Verwendung dieser Kategorien verpflichtend vorgesehen ist. Unternehmen, die bereits über ein etabliertes, beispielsweise nach ISO 27001 zertifiziertes Risikomanagement mit detaillierteren Gefährdungsmodellen verfügen, müssten ihre bestehenden Systeme gegebenenfalls an die Vorgaben der RMMV anpassen. In der Praxis werden Risiken häufig etwa nach Naturereignissen, Strom- und Versorgungsausfällen, Konfigurationsfehlern, Schwachstellen, organisatorischen

Mängeln, menschlichem Fehlverhalten oder unterschiedlichen Angriffsszenarien unterschieden. Eine verpflichtende Umstellung bestehender Risikomethoden oder die parallele Führung mehrerer Klassifizierungssysteme würde zusätzlichen administrativen Aufwand verursachen, ohne einen erkennbaren zusätzlichen Sicherheitsgewinn zu bringen.

Die ISPA regt daher an, klarzustellen, dass die vier Kategorien ausschließlich als übergeordnete Berichts- und Zuordnungsdimensionen dienen und bestehende, gleichwertige Risikotaxonomien uneingeschränkt weiterverwendet werden dürfen, sofern eine nachvollziehbare Zuordnung zu den vier Kategorien hergestellt werden kann. Zudem sollten die Anforderungen der RMMV in bestehende integrierte Risikomanagementsysteme eingebettet und gemeinsam mit anderen gesetzlich erforderlichen Risikoanalysen (z. B. nach RKEG) umgesetzt werden dürfen, ohne dass eine eigenständige NISG-spezifische Parallelmethodik oder eine mehrfache Durchführung inhaltlich gleichwertiger Risikoanalysen erforderlich wird.

Darüber hinaus sollte in der Kategorie „standortbezogene Umweltrisiken“ der unbefugte physische Zutritt externer Personen nicht genannt werden. Aus Sicht der ISPA handelt es sich dabei nicht um eine Umweltgefahr, sondern um ein menschliches Risiko, das systematisch der Kategorie „menschliche Risiken“ zuzuordnen wäre.

2. Ausgleichsmaßnahmen

Der Entwurf sieht verpflichtende Ausgleichsmaßnahmen vor, wenn einzelne Anforderungen unverhältnismäßig oder vorübergehend nicht umsetzbar sind. Dies ist gegenüber der DVO überschießend: ErwGr 5 der DVO spricht lediglich von der Möglichkeit von Ausgleichsmaßnahmen unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit; dieser Möglichkeitscharakter fehlt im Konzept der RMMV. Art 2 Abs 2 DVO sieht demgegenüber ohnehin nur eine Dokumentationspflicht für die Nichtanwendung technischer oder methodischer Anforderungen vor, die nur anzuwenden sind, wenn sie angemessen, anwendbar oder durchführbar sind – eine verpflichtende „Ausgleichsmaßnahme“ kennt die DVO in diesem Zusammenhang nicht.

Unabhängig davon, ob und in welcher Form Ausgleichsmaßnahmen vorgesehen werden, erscheint auch die in den Erläuterungen vorgenommene Anknüpfung an „Größe und vorhandene Ressourcen“ der Einrichtung interpretationsbedürftig. Diese Formulierung birgt die Gefahr, dass bei ressourcenstarken Unternehmen praktisch sämtliche Anforderungen unabhängig von der konkreten Risikosituation umzusetzen wären.

Die ISPA regt daher an, klarzustellen, dass die Verhältnismäßigkeitsprüfung auf einer gesamthaften, risikobasierten Betrachtung beruht und insbesondere folgende Aspekte berücksichtigt:

- 1) mögliche Auswirkungen auf Verfügbarkeit und Versorgungssicherheit,
- 2) konkrete Risikoexposition und Kritikalität der betroffenen Systeme,
- 3) Eintrittswahrscheinlichkeit und potenzielles Schadensausmaß,
- 4) technische und betriebliche Durchführbarkeit,
- 5) Safety-Anforderungen, Lebenszyklus und Herstellerunterstützung der eingesetzten Systeme,
- 6) das durch alternative oder kompensierende Maßnahmen tatsächlich erreichte Sicherheitsniveau sowie
- 7) die Kosten der Umsetzung im Verhältnis zur erzielbaren Risikoreduktion.

Ferner sollte klargestellt werden, wann eine Ausgleichsmaßnahme als ausreichend anzusehen ist. Der Entwurf könnte dahingehend verstanden werden, dass eine kompensierende Maßnahme dasselbe Schutzniveau vollständig erreichen muss; sachgerechter erscheint es, auf eine dem konkreten Risiko angemessene Risikoreduktion abzustellen.

II. Zur Verordnung über die Erheblichkeit von Cybersicherheitsvorfällen (ECV)

1. Böswilliger/unbefugter Zugriff (lit h)

Die DVO verlangt in Bezug auf einen mutmaßlich böswilligen und unbefugten Zugriff, dass dieser geeignet ist, schwerwiegende Betriebsstörungen zu verursachen. Gemäß ECV ist jedoch notwendig, dass ein solcher Zugriff wahrscheinlich dazu führt, schwerwiegende Betriebsstörungen zu verursachen. Diese Abweichung erweitert den Anwendungsbereich des Kriteriums im Vergleich zum unionsrechtlichen Maßstab oder schafft zumindest Rechtsunsicherheit. Die ISPA regt daher an, die verwendete Terminologie an jene der DVO anzugleichen. Dadurch würde klargestellt werden, dass ausschließlich darauf abzustellen ist, ob der Zugriff geeignet ist, schwerwiegende Betriebsstörungen zu verursachen.

2. Konzernweite Vorfälle und Shared-Service-Strukturen

Der Entwurf enthält keine ausdrücklichen Regelungen für konzernweite Vorfälle bzw. zentrale IT-Dienstleisterstrukturen. Unklar bleibt insbesondere, ob und unter welchen Voraussetzungen eine koordinierte oder zentrale Meldung durch einen zentralen IT-Dienstleister bzw. eine dafür benannte Stelle zulässig ist, welche Informationen die betroffenen Einrichtungen im Rahmen einer solchen koordinierten Meldung bereitzustellen haben und wie redundante Mehrfachmeldungen desselben technischen Sachverhalts vermieden werden können. Die ISPA regt hierzu ausdrückliche Klarstellungen an.

3. Beginn der Meldefrist

In der praktischen Vorfallsbearbeitung sind Schadensumfang, Nutzerzahlen, Datenabflüsse und finanzielle Auswirkungen regelmäßig nicht unmittelbar nach Erkennung eines Vorfalls feststellbar. Es sollte daher ausdrücklich klargestellt werden, dass die gesetzlichen Meldefristen nicht bereits mit dem ersten technischen Alarm oder Verdachtsereignis beginnen, sondern erst dann, wenn nach einer qualifizierten Anfangsbewertung mit hinreichender Gewissheit von einem erheblichen Cybersicherheitsvorfall ausgegangen werden kann. Dies entspricht auch den Erwägungen der DVO.

4. Bundesland-Kriterium

Der Entwurf sieht als Erheblichkeitskriterium vor, dass ein Vorfall erheblich sein kann, wenn Dienste im überwiegenden Gebiet zumindest eines Bundeslandes für mehr als 24 Stunden ausfallen oder nur eingeschränkt verfügbar sind. Für klassische, örtlich gebundene Versorgungsleistungen ist ein solcher geografischer Bezug nachvollziehbar; für zentral erbrachte IT-Dienstleistungen, Plattformen, Rechenzentrumsleistungen oder konzernweit genutzte Anwendungen erscheint eine Zuordnung zu Bundeslandgrenzen jedoch häufig nicht sachgerecht. Die ISPA regt an klarzustellen, wann ein Dienst einem bestimmten Bundesland zuzurechnen ist: Ob der Standort der Systeme, der Nutzer oder der Leistungserbringung maßgeblich ist, wie zentral bzw. bundeslandübergreifend erbrachte Dienste zu behandeln sind, und ob für nicht territorial abgrenzbare Dienste alternative Kriterien (z. B. Nutzerzahl, Funktionsumfang, betroffene kritische Geschäftsprozesse) heranzuziehen sind.

5. Aktivierung von Krisen- oder Wiederherstellungsplänen (lit j)

Nach dem Entwurf soll bereits die Aktivierung des Krisenmanagements oder von Notfallwiederherstellungsplänen des Betriebskontinuitätsmanagements einen erheblichen Cybersicherheitsvorfall begründen können. Dieses Kriterium ist Art. 3 DVO fremd und sollte entfallen.

Interne Eskalationsschwellen sind organisationsabhängig: Ein vorsichtiges, gut aufgestelltes Unternehmen aktiviert Krisen- bzw. Wiederherstellungspläne tendenziell früher bzw. vorsorglich – etwa als Ausdruck eines besonders reifen Sicherheits- und Notfallmanagements – und erfüllt damit automatisch das Kriterium eines erheblichen Cybersicherheitsvorfalls, während Organisationen mit weniger ausgereiften Prozessen bzw. höheren Eskalationsschwellen nicht meldepflichtig würden. Die unmittelbare Anknüpfung der Meldepflicht an eine interne Eskalationsentscheidung schafft damit einen Anreiz, interne Pläne möglichst spät zu aktivieren, und bestraft im Ergebnis vorsichtiges Handeln.

Die Aktivierung von Krisenmanagement- oder Wiederherstellungsmaßnahmen sollte daher allenfalls als Indiz für die Schwere eines Vorfalls herangezogen werden können, nicht jedoch als

eigenständiger Auslösetatbestand für eine Meldepflicht.

6. Wiederholte Cybersicherheitsvorfälle

Die Berücksichtigung wiederholter Vorfälle erscheint grundsätzlich nachvollziehbar. Für die praktische Anwendung sollte jedoch klargestellt werden, was unter „derselben offensichtlichen Ursache“ und „demselben Wirkungsbereich“ zu verstehen ist. Unklar ist insbesondere, ob damit etwa derselbe Angreifer, dieselbe Schwachstelle, dieselbe Angriffsmethode oder dasselbe organisatorische Fehlverhalten gemeint ist. Zudem sollte geregelt werden, wann mehrere Ereignisse als zusammenhängende Vorfallsreihe oder als eigenständige Vorfälle gelten. Auch der Begriff „Wirkungsbereich“ bedarf einer näheren Definition, etwa ob damit dasselbe System, derselbe Dienst, derselbe Geschäftsprozess oder dieselbe Gesellschaft gemeint ist. Schließlich sollte klargestellt werden, wie anfallende Kosten zusammenzurechnen sind und ob dies nur innerhalb einer Gesellschaft oder auch über mehrere Gesellschaften bzw. einen zentralen IT-Dienstleister hinweg gilt.

III. Telekom-Netzsicherheitsverordnung

Darüber hinaus fordert die ISPA das **vollständige Außerkrafttreten der Telekom-Netzsicherheitsverordnung (TK-NSiV)**. Das NISG 2026 sieht bereits umfassende Risikomanagement- und Meldepflichten vor, die Betreiber öffentlicher Kommunikationsnetze und -dienste erfassen. Die Erläuterungen zur derzeit konsultierten Risikomanagementmaßnahmen-Verordnung (RMMV) halten zudem ausdrücklich fest, dass mangels Vollzugserfahrungen zum NISG 2026 zunächst auf zusätzliche sektorspezifische Anforderungen verzichtet wird. Erst auf Grundlage praktischer Erfahrungen soll über deren Erforderlichkeit und Ausgestaltung entschieden werden. Eine parallele Anwendung der TK-NSiV würde dieser gesetzgeberischen Wertung widersprechen und zu einer sachlich nicht gerechtfertigten Doppelregulierung führen. Die ISPA fordert daher, die TK-NSiV vollständig außer Kraft zu setzen.

Conclusio

Die Orientierung der Entwürfe an der DVO (EU) 2024/2690 wird von der ISPA ausdrücklich begrüßt. Insgesamt sollte darauf geachtet werden, dass die vorgesehenen Regelungen möglichst klar, verhältnismäßig und praxistauglich ausgestaltet sind und keinen unnötigen zusätzlichen Verwaltungsaufwand verursachen. Die ISPA ersucht daher, die in dieser Stellungnahme angeführten Punkte im weiteren Verfahren zu berücksichtigen, und steht für Rückfragen sowie weiterführende Gespräche jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen



Mag. Stefan Ebenberger
Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 220 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.