

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2026**Ausgegeben am 1. Oktober 2026****Teil II**

290. Verordnung: Netz- und Informationssystemsicherheits-Verordnung

290. Verordnung der Cybersicherheitsbehörde zur Festlegung näherer Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit und weiterer Kriterien über das Vorliegen eines erheblichen Cybersicherheitsvorfalls (Netz- und Informationssystemsicherheits-Verordnung – NISV 2026)

Aufgrund des § 32 Abs. 5 und § 35 Abs. 3 des Netz- und Informationssystemsicherheitsgesetzes 2026 (NISG 2026), BGBl. I Nr. 94/2025, wird verordnet:

Inhaltsverzeichnis

1. Abschnitt

Allgemeine Bestimmungen

§ 1. Gegenstand

2. Abschnitt

Risikomanagementmaßnahmen

§ 2. Anforderungen an Risikomanagementmaßnahmen

§ 3. Risikokategorien

§ 4. Kompensierende Maßnahmen

3. Abschnitt

Erheblichkeit von Cybersicherheitsvorfällen

§ 5. Erhebliche Cybersicherheitsvorfälle

§ 6. Planmäßige Betriebsunterbrechungen

§ 7. Wiederholte Cybersicherheitsvorfälle

4. Abschnitt

Schlussbestimmungen

§ 8. Verweisungen

§ 9. Inkrafttreten

1. Abschnitt

Allgemeine Bestimmungen

Gegenstand

§ 1. Mit dieser Verordnung werden

1. nähere Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sowie

2. weitere Kriterien über das Vorliegen eines erheblichen Cybersicherheitsvorfalls

festgelegt.

2. Abschnitt

Risikomanagementmaßnahmen

Anforderungen an Risikomanagementmaßnahmen

§ 2. Die näheren Anforderungen an die Risikomanagementmaßnahmen 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, sind auch auf die nicht von dieser Durchführungsverordnung umfassten in den Anlagen 1 und 2 des Netz- und Informationssystemssicherheitsgesetzes 2026 (NISG 2026), BGBl. I Nr. 94/2025, gelisteten Arten wesentlicher und wichtiger Einrichtungen anwendbar.

Risikokategorien

§ 3. Wesentliche und wichtige Einrichtungen haben sich im Zuge ihrer Risikoanalyse zumindest an folgenden Risikokategorien zu orientieren und bei ihrem Risikomanagementverfahren im Bereich der Cybersicherheit zu berücksichtigen:

1. technologische Risiken,
2. menschliche Risiken,
3. Risiken in der IKT-Lieferkette,
4. standortbezogene Risiken für Netz- und Informationssysteme.

Kompensierende Maßnahmen

§ 4. (1) Kompensierende Maßnahmen sind umzusetzen, wenn eine wesentliche oder wichtige Einrichtung einzelnen Anforderungen gemäß § 2 vorübergehend oder aufgrund ihrer Größe nicht entsprechen kann.

(2) Kompensierende Maßnahmen müssen geeignet sein, dem jeweiligen Zweck einer Anforderung gemäß § 2 und der Minimierung damit verbundener Risiken auf Basis einer Risikobewertung zu dienen.

(3) Die Umsetzung kompensierender Maßnahmen ist nachvollziehbar und begründet zu dokumentieren. Die Wirksamkeit kompensierender Maßnahmen ist in regelmäßigen Abständen, jedoch zumindest jährlich, zu überprüfen.

(4) Die Pflicht zur Umsetzung kompensierender Maßnahmen besteht nicht bezüglich jener Anforderungen gemäß § 2, denen ausdrücklich nur soweit angemessen, anwendbar oder durchführbar zu entsprechen ist.

3. Abschnitt

Erheblichkeit von Cybersicherheitsvorfällen

Erhebliche Cybersicherheitsvorfälle

§ 5. (1) Ein Cybersicherheitsvorfall gilt in Bezug auf die betreffenden Einrichtungen jedenfalls als erheblich im Sinne von § 35 Abs. 1 NISG 2026, wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

1. der Cybersicherheitsvorfall hat der betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert niedriger ist – verursacht oder kann einen solchen Verlust verursachen;
2. der Cybersicherheitsvorfall hat den Abfluss von Geschäftsgeheimnissen der betreffenden Einrichtung im Sinne von § 26b des Bundesgesetzes gegen den unlauteren Wettbewerb 1984 (UWG), BGBl. Nr. 448/1984, oder von Informationen, die gemäß § 6 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG), BGBl. I Nr. 5/2024, der Geheimhaltung unterliegen, verursacht oder kann einen solchen Abfluss verursachen;
3. der Cybersicherheitsvorfall hat den Tod einer natürlichen Person verursacht oder kann einen solchen Tod verursachen;

4. der Cybersicherheitsvorfall hat eine schwere Schädigung der Gesundheit einer natürlichen Person verursacht oder kann eine solche Schädigung verursachen;
5. es hat einen erfolgreichen, mutmaßlich böswilligen und unbefugten Zugriff auf Netz- und Informationssysteme gegeben, der wahrscheinlich dazu führt, schwerwiegende Betriebsstörungen zu verursachen;
6. der Cybersicherheitsvorfall erfüllt die in § 7 aufgeführten Kriterien für wiederholte Cybersicherheitsvorfälle;
7. der Cybersicherheitsvorfall hat zum Ausfall oder zur eingeschränkten Verfügbarkeit der von der Einrichtung erbrachten Dienste für mehr als 100 000 Nutzer oder 10 % der Nutzer – je nachdem, welcher Wert niedriger ist – für mehr als 24 Stunden geführt oder kann dazu führen (Ausbreitung auf Nutzer). Eine eingeschränkte Verfügbarkeit liegt insbesondere dann vor, wenn ein von einer betreffenden Einrichtung erbrachter Dienst nicht im regelmäßig zu erwartenden Umfang erbracht werden kann;
8. der Cybersicherheitsvorfall hat 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 oder kann dazu führen (geografische Ausbreitung). Eine eingeschränkte Verfügbarkeit liegt insbesondere dann vor, wenn ein von einer betreffenden Einrichtung erbrachter Dienst nicht im regelmäßig zu erwartenden Umfang erbracht werden kann;
9. der Cybersicherheitsvorfall hat zur Aktivierung des Krisenmanagements oder von Notfallwiederherstellungsplänen des Betriebskontinuitätsmanagements geführt.

Planmäßige Betriebsunterbrechungen

§ 6. Planmäßige Betriebsunterbrechungen und geplante Folgen planmäßiger Wartungsarbeiten, die von oder im Auftrag der betreffenden Einrichtung durchgeführt werden, gelten nicht als erhebliche Cybersicherheitsvorfälle.

Wiederholte Cybersicherheitsvorfälle

§ 7. Cybersicherheitsvorfälle, die einzeln betrachtet nicht als erhebliche Cybersicherheitsvorfälle anzusehen sind, gelten zusammengekommen als ein erheblicher Cybersicherheitsvorfall, wenn sie alle folgenden Kriterien erfüllen:

1. sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten;
2. sie haben dieselbe offensichtliche Ursache und Auswirkung;
3. sie erfüllen zusammengekommen die in § 5 Abs. 1 Z 1 aufgeführten Kriterien.

4. Abschnitt

Schlussbestimmungen

Verweisungen

§ 8. Soweit in dieser Verordnung auf Bundesgesetze verwiesen wird, ist die zum Zeitpunkt des Inkrafttretens der Verordnung geltende Fassung maßgeblich.

Inkrafttreten

§ 9. Diese Verordnung tritt mit Ablauf des Tages der Kundmachung in Kraft.

Kasinger

	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2026-10-01T16:15:32+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.