

Kurztitel

Netz- und Informationssystemsicherheitsgesetz 2026

Kundmachungsorgan

BGBI. I Nr. 94/2025

Typ

BG

§/Artikel/Anlage

§ 3

Inkrafttretensdatum

01.10.2026

Abkürzung

NISG 2026

Index

41/01 Sicherheitsrecht

Text**Begriffsbestimmungen**

§ 3. Im Sinne dieses Bundesgesetzes bedeutet

1. „Netz- und Informationssystem“
 - a) ein Kommunikationsnetz gemäß § 4 Z 1 des Telekommunikationsgesetzes 2021 (TKG 2021), BGBI. I Nr. 190/2021,
 - b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
 - c) digitale Daten, die von den in lit. a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;
2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen können;
3. „Cybersicherheit“ alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;
4. „öffentliches Kommunikationsnetz“ ein öffentliches elektronisches Kommunikationsnetz gemäß § 4 Z 9 TKG 2021;
5. „Kommunikationsdienst“ ein elektronischer Kommunikationsdienst gemäß § 4 Z 4 TKG 2021;
6. „IKT-Produkt“ ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;

7. „IKT-Dienst“ ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;
8. „IKT-Prozess“ jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;
9. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;
10. „Einrichtung“ eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person oder eingetragene Personengesellschaft, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;
11. „Leitungsorgan“ eine oder mehrere natürliche Personen oder Verwaltungsorgane, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung berufen sind;
12. „DNS-Diensteanbieter“ (Domainnamensystem – DNS) eine Einrichtung, die
 - a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domännennamen anbietet, oder
 - b) autoritative Dienste zur Auflösung von Domännennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namensservern, anbietet;
13. „Namenregister der Domäne oberster Stufe“ oder „TLD-Namenregister“ eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domännennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namensserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namensserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;
14. „Einrichtung, die Domännennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa Wiederverkäufer oder Anbieter von Datenschutz- oder Proxy-Registrierungsdiensten;
15. „Anbieter digitaler Dienste“ eine juristische Person oder eingetragene Personengesellschaft, die einen digitalen Dienst gemäß § 3 Z 1 des E-Commerce-Gesetzes (ECG), BGBl. I Nr. 152/2001, erbringt, bei dem es sich um einen Online-Marktplatz oder eine Online-Suchmaschine oder eine Plattform für Dienste sozialer Netzwerke handelt;
16. „Vertrauensdienst“ ein Vertrauensdienst gemäß Art. 3 Z 16 der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 23 vom 29.01.2015 S. 19;
17. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter gemäß Art. 3 Z 19 Verordnung (EU) Nr. 910/2014;
18. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter gemäß Art. 3 Z 20 Verordnung (EU) Nr. 910/2014;
19. „qualifizierte elektronische Signaturerstellungseinheit“ eine qualifizierte elektronische Signaturerstellungseinheit gemäß Art. 3 Z 23 Verordnung (EU) Nr. 910/2014;
20. „qualifizierte elektronische Siegelerstellungseinheit“ eine qualifizierte elektronische Siegelerstellungseinheit gemäß Art. 3 Z 32 Verordnung (EU) Nr. 910/2014;
21. „Konformitätsbewertungsbericht“ ein Konformitätsbewertungsbericht gemäß Art. 20 Abs. 1 Verordnung (EU) Nr. 910/2014;
22. „vertrauenswürdige Systeme eines Vertrauensdiensteanbieters“ Systeme und Produkte, die den Erfordernissen gemäß Art. 24 Abs. 2 lit. e und f Verordnung (EU) Nr. 910/2014 entsprechen;
23. „Anbieter verwalteter Dienste“ (Managed Service Provider) eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, dies entweder in den Räumlichkeiten der Kunden oder aus der Ferne;
24. „Anbieter verwalteter Sicherheitsdienste“ ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;
25. „Vertreter“ eine in der Europäischen Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung,

die Domännennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltzustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der oder die nicht in der Europäischen Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT – statt an die Einrichtung – hinsichtlich der Pflichten dieser Einrichtung gemäß diesem Bundesgesetz wenden kann;

26. „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Cybersicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Cybersicherheitsvorfalls zum Ausdruck gebracht wird;
27. „Cyberbedrohung“ ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;
28. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht;
29. „Beinahe-Cybersicherheitsvorfall“ (Near Miss) 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 haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder das nicht eingetreten ist;
30. „Cybersicherheitsvorfall“ 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;
31. „Cybersicherheitsvorfall großen Ausmaßes“ ein Cybersicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats der Europäischen Union übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat;
32. „Innerer Kreis der Operativen Koordinierungsstruktur“ (IKDOK) eine Struktur zur Koordination auf operativer Ebene im Bereich der Cybersicherheit bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, der Cybersicherheitsbehörde, des Bundesministers für Landesverteidigung sowie des Bundesministers für europäische und internationale Angelegenheiten;
33. „Operative Koordinierungsstruktur“ (OpKoord) eine Struktur zur Koordination auf operativer Ebene im Bereich der Cybersicherheit bestehend aus dem IKDOK und den Computer-Notfallteams (CSIRTs), die anlassbezogen um zusätzliche Teilnehmer erweitert werden kann;
34. „Kooperationsgruppe“ ein gemäß Art. 14 der Richtlinie (EU) 2022/2555 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. Nr. L 333 vom 27.12.2022 S. 80, eingesetztes Gremium zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten der Europäischen Union und zur Stärkung des Vertrauens;
35. „CSIRTs-Netzwerk“ das gemäß Art. 15 NIS-2-Richtlinie errichtete Netzwerk der CSIRTs der Mitgliedstaaten der Europäischen Union;
36. „EU-CyCLONe“ das gemäß Art. 16 NIS-2-Richtlinie zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Europäischen Union eingerichtete Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crisis Liaison Organisation Network, kurz: EU-CyCLONe);
37. „Überwachungsbeauftragter“ ein Mitarbeiter der Cybersicherheitsbehörde, der für den gemäß § 39 Abs. 3 Z 2 festgelegten Zeitraum die Einhaltung der Risikomanagementmaßnahmen (§ 32) und der Berichtspflichten (§ 34) einer wesentlichen Einrichtung überprüft.

Schlagworte

Netzsystem, Datenschutzdienst

Zuletzt aktualisiert am

30.12.2025

Gesetzesnummer

20013065

Dokumentnummer

NOR40273862