

Positionspapier NISG 2026
für den Teilsektor
„Anbieter von
Rechenzentrumsdiensten“

Version 1
26.4.2026



NISG 2026

Gender-Hinweis: Die in Folge gewählte männliche Form bezieht sich immer zugleich auf weibliche, männliche und diverse Personen. Auf eine Mehrfachbezeichnung wird zugunsten der besseren Lesbarkeit verzichtet.

Inhalt

Prolog	4
Management Summary	4
1 NISG 2026 und die Auswirkung auf „Anbieter von Rechenzentrumsdiensten“	6
1.1 Allgemeines	6
1.2 NISG 2026 Begriffsbestimmung „Rechenzentrumsdienst“ und Abgrenzungen	7
1.2.1 Abgrenzung Sektor „Rechenzentrumsdienst“ zu anderen Sektoren und Teilsektoren	7
1.2.2 Dienstumfang im Sektor „Rechenzentrumsdienste“ laut Begriffsbestimmung	8
1.3 NISG 2026 Registrierungspflicht für betroffene wesentliche und wichtige Einrichtungen	9
1.3.1 Allgemeines zur NISG 2026 Registrierungspflicht	9
1.3.2 Kriterien für die NISG 2026 Registrierungspflicht im Teilsektor „Rechenzentrumsdienste“	10
2 Netz- und Informationssysteme für die Erbringung von Rechenzentrumsdiensten	12
2.1 Allgemeines zu Netz- und Informationssystemen im NISG 2026 Scope	12
2.2 Eingebettete Netz- und Informationssysteme in der physischen RZ-Basisinfrastruktur	13
3 Anforderung für Risikomanagementmaßnahmen im Bereich der Cybersicherheit	15
3.1 Risikomanagementmaßnahmen gemäß § 32 NISG 2026	15
3.2 Nachweis der Wirksamkeit von Risikomanagementmaßnahmen	16
3.2.1 Selbstdeklaration	16
3.2.2 Prüfung durch unabhängige Stelle	17
3.2.3 Anlassbezogene Kontrollen durch die Cybersicherheitsbehörde	18
4 Ausblick auf die Weiterentwicklung dieses Positionspapiers	19

Prolog

Die Austrian Data Center Association „ADCA“ (www.austriandatacenter.org) ist ein gemeinnütziger Verein, der sich als Interessensvertretung österreichischer Rechenzentrumsbetreiber begreift. Rechenzentren sind das Herz der Digitalisierung: Ob Finanzdienstleister, Bauunternehmen, Telekommunikationsanbieter, Betriebe, in denen Remote Working praktiziert wird, oder kritische Infrastruktur – ohne hochverfügbare Rechenzentren (Data Center) und den Einrichtungen, die diese Rechenzentren betreiben, funktionieren weite Teile von Wirtschaft und Gesellschaft heute nicht mehr.

Im NISG 2026 werden „Anbieter von Rechenzentrumsdienstleistungen“ explizit als Sektor mit hoher Kritikalität adressiert. Weiters wird an unterschiedlichen Stellen im NISG 2026 die geforderte Zusammenarbeit mit maßgeblichen Interessenträgern und die Verpflichtung zur Pflege von Kooperationsbeziehungen mit diesen einschlägigen Interessenträgern beschrieben. Die ADCA bietet sich für den Teilsektor „Rechenzentrumsdienstleistungen“ als einschlägiger Interessenträger an und nimmt mit ihrem breit aufgestellten Know-how aus der österreichischen Rechenzentrumsbranche und dem diesbezüglichen Stand der Technik diese Aufgabe gerne wahr.

Management Summary

Mit dem in Kraft tretenden NISG 2026 fallen Betreiber von Rechenzentren, die als betroffene Einrichtung ihre Rechenzentrumsdienste nicht nur ausschließlich für sich selbst nutzen, ab dem 1. Oktober 2026 nun umfassend unter die gesetzlichen Pflichten für Cybersicherheit in Österreich. Der Betrieb von Rechenzentrumsdiensten wird dabei als Teilsektor des Bereichs „Digitale Infrastruktur“ mit hoher Kritikalität eingestuft und unterliegt damit besonderen regulatorischen Anforderungen. Entscheidend für den Umfang der Verpflichtungen ist die Einstufung als wesentliche oder wichtige Einrichtung aufgrund der qualitativen Merkmale des Rechenzentrumsdienstleistungsbündels und der Unternehmensgröße. Große Unternehmen gelten grundsätzlich als wesentliche Einrichtungen, mittlere Unternehmen als wichtige Einrichtungen. Zusätzlich kann aufgrund der besonderen Bedeutung eines Unternehmens für die Versorgungssicherheit eine behördliche Einstufung unabhängig von der Unternehmensgröße erfolgen. Für betroffene Unternehmen ergeben sich insbesondere Verpflichtungen hinsichtlich Registrierung, Risikomanagementmaßnahmen, Sicherheitsvorfällen, Nachweispflichten und behördlicher Aufsicht.

Das vorliegende Positionspapier der ADCA erläutert die Auswirkungen des NISG 2026 auf Anbieter von Rechenzentrumsdiensten und schafft Orientierung bei der praktischen Umsetzung der neuen gesetzlichen Anforderungen.

Begriffsbestimmung und Abgrenzung

Im Mittelpunkt steht zunächst die Definition des Begriffs „Rechenzentrumsdienst“. Dieser umfasst die zentrale Unterbringung von IT- und Netzausrüstung, die Bereitstellung von Verbindungsinfrastrukturen, die Energieversorgung und -verteilung sowie die Sicherstellung geeigneter Umgebungsbedingungen, insbesondere durch Klimatisierung. Der Gesetzgeber orientiert sich dabei stark an der europäischen Normenreihe EN 50600. Nicht jeder Standort mit IT-Infrastruktur fällt automatisch unter diese Definition. Entscheidend ist vielmehr, dass ein speziell für Rechenzentrumszwecke ausgelegtes Dienstleistungsbündel angeboten wird.

Registrierungspflicht

Ein wesentlicher Schwerpunkt des Positionspapiers liegt auf der Frage, welche Unternehmen tatsächlich registrierungspflichtig werden. Betreiber von Rechenzentrumsdiensten müssen sich grundsätzlich bei der Cybersicherheitsbehörde registrieren, wenn sie die gesetzlichen Kriterien erfüllen und als wesentliche oder wichtige Einrichtung einzustufen sind. Hervorgehoben wird, dass keine automatische „Vererbung“ der NISG-Pflichten von Kunden auf Rechenzentrumsbetreiber stattfindet. Die Beurteilung erfolgt stets auf Ebene jener Einrichtung, die den Rechenzentrumsdienst tatsächlich erbringt.

Sachlicher Anwendungsbereich

Das Positionspapier schafft darüber hinaus Klarheit hinsichtlich jener Netz- und Informationssysteme, die sich in der Verwaltungshoheit des Rechenzentrumsbetreibers befinden und für die Erbringung der angebotenen Dienstleistungen erforderlich sind. Dazu zählen nicht nur klassische IT-Systeme, sondern insbesondere auch sogenannte OT-Systeme wie eingebettete digitale Steuerungs- und Überwachungssysteme innerhalb der Rechenzentrumsinfrastruktur. Diese Systeme gelten als sicherheitskritisch, da ihre Kompromittierung die Verfügbarkeit, Integrität oder Vertraulichkeit der Rechenzentrumsdienstleistungen unmittelbar beeinträchtigen kann.

Risikomanagement

Im Bereich der Risikomanagementmaßnahmen verweist das Positionspapier auf die umfassenden Anforderungen des § 32 NISG 2026 sowie auf die unmittelbar anwendbare Durchführungsverordnung (EU) 2024/2690. Betroffene Einrichtungen müssen geeignete technische, organisatorische und operative Maßnahmen umsetzen, um Cyberrisiken wirksam zu identifizieren, zu bewerten und zu reduzieren. Grundlage aller Maßnahmen ist ein risikobasierter Ansatz unter Berücksichtigung des Standes der Technik sowie einschlägiger Normen und Standards.

Nachweis

Ein weiterer Punkt betrifft den Nachweis der Wirksamkeit dieser Maßnahmen. Innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht müssen betroffene Einrichtungen eine strukturierte Selbstdeklaration gegenüber der Cybersicherheitsbehörde abgeben. Darüber hinaus können unabhängige Prüfungen verlangt werden. Als besonders relevante Nachweise werden Zertifizierungen nach ISO/IEC 27001 für Informationssicherheitsmanagement sowie nach EN 50600 für Rechenzentrumsinfrastrukturen genannt. Zusätzlich verfügt die Cybersicherheitsbehörde über weitreichende Aufsichts- und Kontrollbefugnisse, die von Informationsanforderungen über Vor-Ort-Kontrollen bis hin zu anlassbezogenen Prüfungen reichen.

Fazit

Das Positionspapier macht deutlich, dass Betreiber von Rechenzentrumsdiensten bereits vor Inkrafttreten des NISG 2026 die notwendigen organisatorischen, technischen und rechtlichen Vorbereitungen treffen sollten. Insbesondere die Identifikation relevanter Systeme, die Durchführung von Risikoanalysen, die Dokumentation bestehender Sicherheitsmaßnahmen sowie die Vorbereitung auf Registrierungs- und Nachweispflichten sollten frühzeitig erfolgen.

Abschließend weist die ADCA darauf hin, dass das vorliegende Dokument den Beginn einer fortlaufenden fachlichen Auseinandersetzung mit den Anforderungen des NISG 2026 darstellt. In künftigen Versionen des Positionspapiers werden weitere wichtige Themen vertieft behandelt, darunter der Stand der Technik und einschlägige Normen für Rechenzentrumsdienste, die praktische Umsetzung der Anforderungen aus der Durchführungsverordnung (EU) 2024/2690, konkrete Ansätze für Risikomanagementmaßnahmen, die Meldung erheblicher Sicherheitsvorfälle sowie weitere regulatorische Anforderungen. In weiteren Schritten werden zusätzliche praxisrelevante Orientierungshilfen und wichtige Informationen für die Umsetzung der gesetzlichen Vorgaben bereitgestellt.

1 NISG 2026 und die Auswirkung auf „Anbieter von Rechenzentrumsdiensten“

1.1 Allgemeines

Das **Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026)** mit seinen wesentlichen inhaltlichen Anforderungen tritt in Österreich am 1. Oktober 2026 in Kraft. Es ersetzt das bisherige Netz- und Informationssicherheitsgesetz (NISG) und dient der Umsetzung der EU Richtlinie 2022/2555 (NIS-2-RL) für festzulegende **Maßnahmen**, mit denen ein **hohes Cybersicherheitsniveau**, insbesondere von wesentlichen und wichtigen Einrichtungen in bestimmten **Sektoren** und den zugehörigen Teilsektoren erreicht werden soll. In dem mit **hoher Kritikalität** eingestuften Sektor „**Digitale Infrastruktur**“ (Z 8 Anhang I NIS-2-RL) befindet sich unter anderem der **Teilsektor „Anbieter von Rechenzentrumsdiensten“**.

Die erwähnten festzulegenden Maßnahmen können von der Cybersicherheitsbehörde in einer Verordnung weiter spezifiziert werden (§ 32 Abs 5 NISG 2026). Für die Sektoren „Digitale Dienste“ und „Digitale Infrastruktur“ und damit auch für den Teilsektor „Anbieter von Rechenzentrumsdiensten“ sind dabei jedoch zum Zweck der Harmonisierung in allen EU-Ländern bereits jene Maßnahmen unmittelbar gültig und wirksam, welche mit der Durchführungsverordnung (EU) 2024/2690 auf Grundlage der Artikel 21 (5), 23 (11) NIS-2-RL bestimmt wurden.

Von EU-Richtlinie zu österreichischem Recht

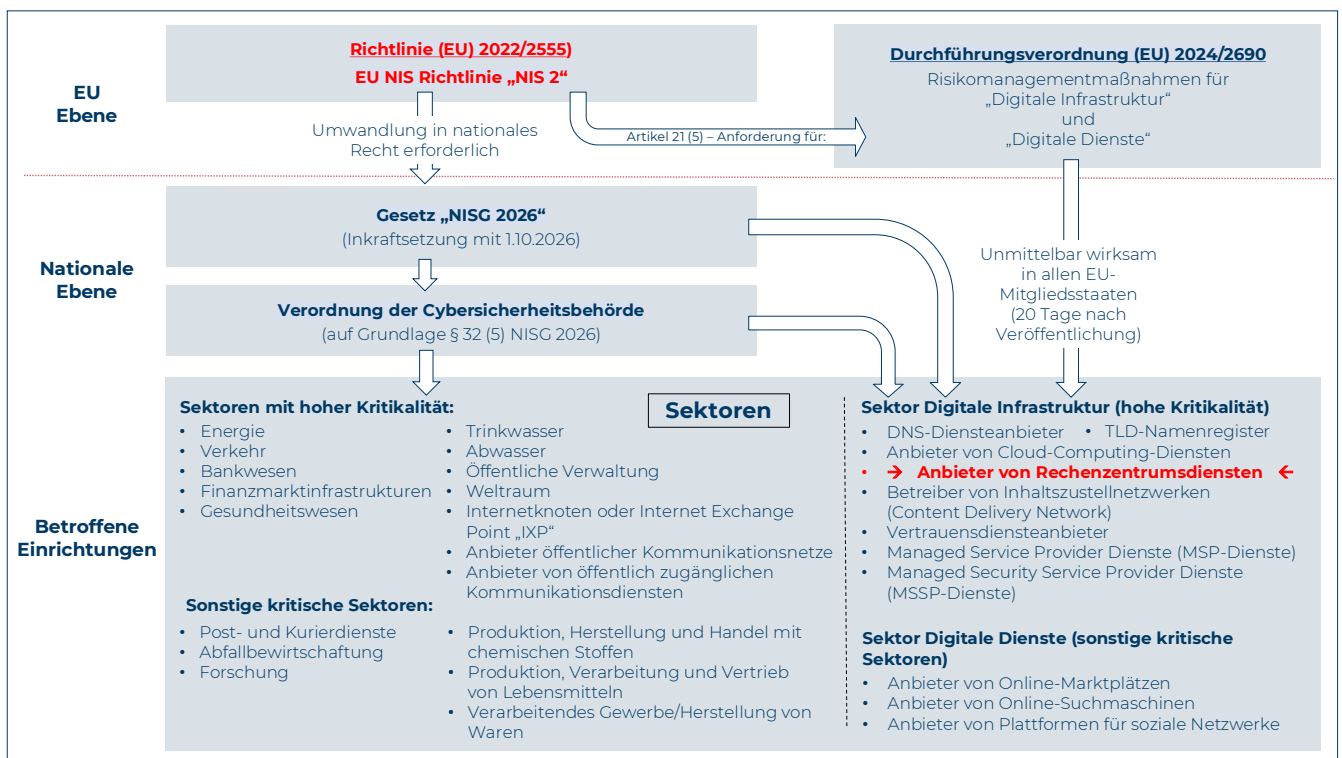


Abbildung 1: NIS 2 Regulatorium und Umsetzung in Österreich

© Peter Wörgötter/Cis-Cert

Gemäß § 32 (1) NISG 2026 haben betroffene wesentliche und wichtige Einrichtungen – darunter also auch **betroffene „Anbieter von Rechenzentrumsdiensten“** – **geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen**. Um die Risiken für die Netz- und Informationssysteme, die sie für den Betrieb oder für die Erbringung ihrer Dienste nutzen, zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

1.2 NISG 2026 Begriffsbestimmung „Rechenzentrumsdienst“ und Abgrenzungen

1.2.1 Abgrenzung Sektor „Rechenzentrumsdienst“ zu anderen Sektoren und Teilsektoren

In Artikel 6 NIS-2-RL sind die für den Zweck der Richtlinie geltenden Definitionen für bestimmte Begriffe festgelegt worden. Diese Begriffsbestimmungen wurden im Wesentlichen im NISG 2026 übernommen. Der für dieses Positionspapier relevante Begriff „Rechenzentrumsdienst“ sowie dessen Abgrenzung zu den anderen im NISG 2026 festgelegten Teilsektoren werden nachfolgend dargelegt.

NOTIZ

„Rechenzentrumsdienst“ bezeichnet laut NISG 2026 einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden (vgl. Anlage 1 zum NISG 2026).

Bei genauerer Betrachtung ist zu erkennen, dass die im NISG 2026 verwendete Begriffsbestimmung für den „Rechenzentrumsdienst“, gleich wie ihre unionsrechtliche Grundlage in der NIS-2-RL, ziemlich wortgetreu mit der Begriffsbestimmung für Rechenzentren aus der EN 50600 Serie übereinstimmt, welche als einschlägige europäische Norm für qualitative Anforderungen an Rechenzentren (Baukonstruktion, technische Ausrüstung sowie Betrieb) anzusehen ist.

Abbildung 2 veranschaulicht die in der Begriffsbestimmung festgelegten Teildienstleistungen für betroffene Einrichtungen im Teilsektor „Rechenzentrumsdienst“, im Kontext mit den anderen Sektoren in der Anlage 1 und Anlage 2 des NISG 2026. Sie zeigt, dass im NISG 2026 der Sektor „Rechenzentrumsdienst“ als RZ-Basisinfrastrukturdienstleistungsbündel etwas anders behandelt wird als die anderen Sektoren. RZ-Betreiber sollten daher auch diesen Teilsektor im Auge behalten:

Worin sich der Teilsektor „Rechenzentrumsdienst“ unterscheidet

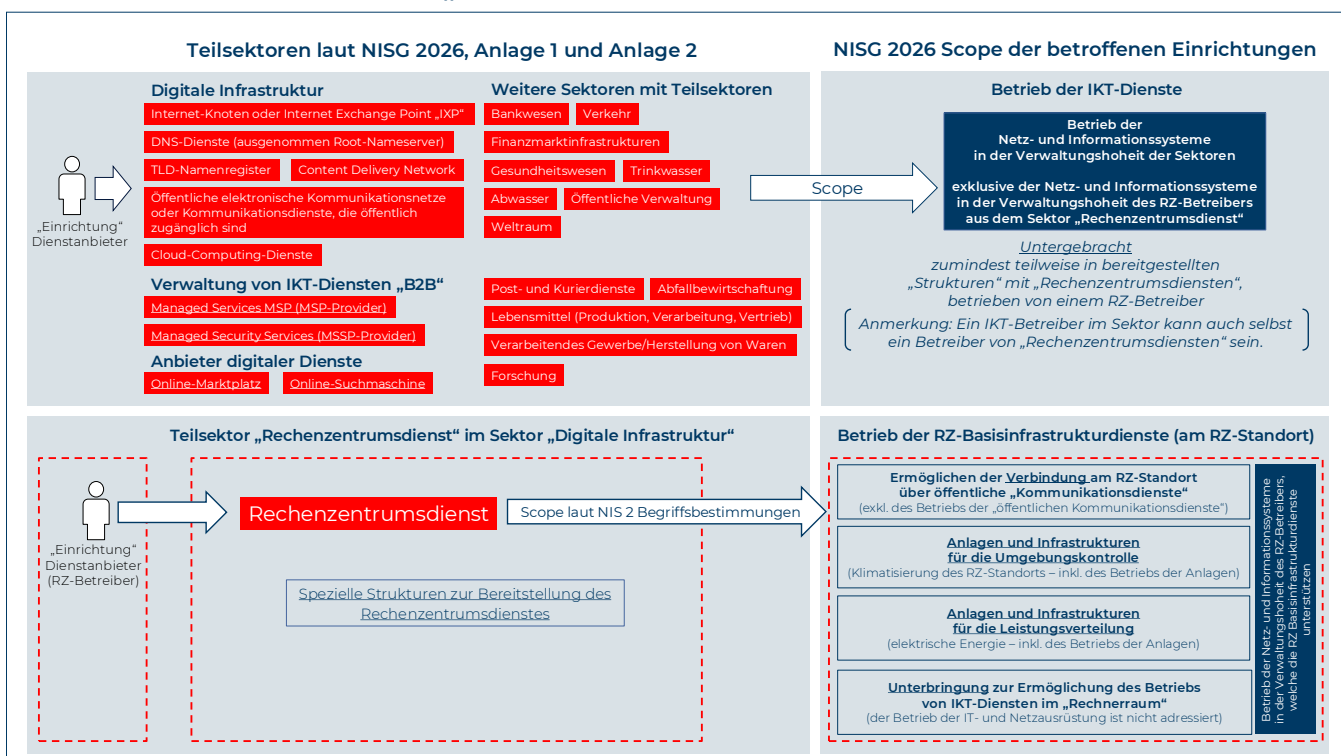


Abbildung 2: Teilsektor „Rechenzentrumsdienst“ im Kontext mit den anderen Sektoren im NISG 2026

© Peter Wörgötter/Cis-Cert

1.2.2 Dienstumfang im Sektor „Rechenzentrumsdienste“ laut Begriffsbestimmung

Bei der Betrachtung aller Sektoren und Teilsektoren im NISG 2026 und der Begriffsbestimmung wird klar, dass unter dem Teilsektor „Anbieter von Rechenzentrumsdiensten“ ein besonderes Bündel von Hauptleistungen (Stichwort „Serverhotel“), das am Markt angeboten werden soll, zu verstehen ist. Auf dieser Grundlage muss daher ein entsprechendes Leistungsbündel vorliegen und vom Anbieter bezweckt worden sein, welches alle gesetzlichen Merkmale eines „Rechenzentrumsdiensts“ erfüllt. Es erscheint daher naheliegend, dass der Zweck des Anbots eines (im Sinne des NISG 2026) „Rechenzentrumsdienstes“ auf die Erfüllung der Nachfrage nach solchen Diensten ausgerichtet sein muss. Von einer Nachfrageerfüllung nach „Rechenzentrumsdiensten“ dürfte beispielsweise wohl dann keine Rede mehr sein, wenn eine bloße Vermietung von reinen Büroräumlichkeiten in Wohn-/Geschäftsgebäuden erfolgt und mit dieser Tätigkeit nicht unmittelbar das gesetzlich definierte Dienstleistungsbündel verfolgt wird. Vor diesem Hintergrund ist darunter der folgende Dienstumfang zu verstehen:

- >> **Zentrale Unterbringung** → die Bereitstellung von speziellen Strukturen oder Gruppen von Strukturen – also Gebäude oder Gebäudeteile und sonstige bauliche Einrichtungen –, die auf die zentrale Unterbringung von IT- und Netzausrüstung ausgelegt sind.

Über die Unterbringung wird der Betrieb von zentraler IT- und Netzausrüstung zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten im Rechneraumbereich des RZ-Standorts angemessen ermöglicht. Der Betrieb der IT- und Netzausrüstung im Rechnerraumbereich des RZ-Standortes selbst (also der Betrieb der IKT-Produkte bzw. die Bereitstellung der IKT-Dienste der Kunden des RZ-Betreibers) ist nicht dem NIS 2026 Teilsektor „Rechenzentrumsdienste“ zuzurechnen, sondern ggf. anderen NISG 2026 Teilsektoren.

Ein als „spezielle Strukturen“ bezeichneter RZ-Standort kann entweder ein reiner Zweckbau sein oder Teil eines Multifunktionsgebäudes (z. B. ein RZ-Standort sowie auch ein Bürostandort). Soll ein „Rechenzentrumsdienst“ (im Sinne des NISG 2026) an einem Standort begründet werden, dann bieten sich für die entsprechende Abgrenzung der relevanten und nicht relevanten Funktionsbereiche die Festlegungen aus der EN 50600-1, Teil „Überblick über die Auslegung von Rechenzentren“ an.

Eine besondere Zweckbestimmung dieser „speziellen Strukturen“ auf den Rechenzentrumsbetrieb ist Voraussetzung, die jedenfalls bei einem nach dem Stand der Technik errichteten RZ-Standort als erfüllt anzusehen ist. Beispielsweise wird entscheidend sein, ob überhaupt ein spezieller Raumbereich zur Aufnahme der IT-Ausrüstung der Kunden vorgesehen ist (ein sogenannter „Rechnerraum“ laut der Begriffsbestimmung in der EN 50600-1), der qualitativ in baulicher und technischer Hinsicht durch den „Anbieter von Rechenzentrumsdiensten“ entsprechend ertüchtigt wurde. Demnach dürfte die bloße Möglichkeit, dass ein Mieter IT-Ausrüstung in seine gemieteten Räumlichkeiten einbringt und darin betreibt, für sich genommen nicht ausreichen, damit der Vermieter das Merkmal der Bereitstellung einer zentralen Unterbringung dieser IT-Ausrüstung im Sinne eines angebotenen „Rechenzentrumsdiensts“ erfüllt hat.

- >> **Verbindung** → die Bereitstellung der entsprechenden Infrastruktur für die Telekommunikationsverkabelung, zur datentechnischen Verbindung der im Rechnerraumbereich des RZ-Standorts untergebrachten IT- und Netzausrüstung der Kunden des RZ-Betreibers mit der Standort-Außenwelt.

Es handelt sich also um die Ermöglichung von „Kommunikationsdiensten“ für die Kunden des RZ-Betreibers am RZ-Standort. Der Betrieb aber der IT- und Netzausrüstung für diese „Kommunikationsdienste“ selbst ist nicht im Teilsektor „Rechenzentrumsdienste“ enthalten, sondern im separaten Teilsektor „Kommunikationsdienste“.

- >> **Anlagen und Infrastrukturen für die Leistungsverteilung** → die Bereitstellung der Energieversorgung und Energieverteilung für die im Rechnerraumbereich am RZ-Standort untergebrachte IT- und Netzausrüstung der Kunden des RZ-Betreibers. Der Betrieb der Anlagen und Infrastrukturen für die Leistungsverteilung am RZ-Standort ist im NIS 2026 Teilsektor „Rechenzentrumsdienste“ enthalten inkl. der diesbezüglich eingesetzten Netz- und Informationssysteme.
- >> **Anlagen und Infrastrukturen für die Umgebungskontrolle** → die Bereitstellung der entsprechenden Umgebungsbedingungen (Klimatisierung) für die am RZ-Standort untergebrachte IT- und Netzausrüstung der Kunden des RZ-Betreibers. Daraus ist als wesensrelevanter Kern dieser Bereitstellung von Klimatisierung abzuleiten, dass geeignete klimatische Umweltbedingungen für den Betrieb der IT-Ausrüstung geschaffen und gesteuert werden müssen. Der Betrieb der Anlagen und Infrastrukturen für die Umgebungskontrolle (Klimatisierung) am RZ-Standort ist im NIS 2026 Teilsektor „Rechenzentrumsdienste“ enthalten inkl. der diesbezüglich eingesetzten Netz- und Informationssysteme.

1.3 NISG 2026 Registrierungspflicht für betroffene wesentliche und wichtige Einrichtungen

1.3.1 Allgemeines zur NISG 2026 Registrierungspflicht

Betroffene wesentliche und wichtige Einrichtungen in Österreich im Sektor „Anbieter von Rechenzentrumsdiensten“ müssen sich ab dem 1. Oktober 2026 bei der Cybersicherheitsbehörde registrieren, sofern sie

- a. ihre Hauptniederlassung* in Österreich haben oder
- b. sie weder in Österreich noch in einem anderen Mitgliedsstaat der Europäischen Union eine Niederlassung haben, aber Dienste in Österreich anbieten, und weder der Cybersicherheitsbehörde in Österreich noch einem anderen Mitgliedsstaat der Europäischen Union einen Vertreter mit Hauptwohnsitz im Inland oder einen Zustellungsbevollmächtigten gemäß § 9 des Zustellgesetzes (ZustG) namhaft gemacht haben.

Als Hauptniederlassung wird jeweils die Niederlassung in demjenigen Mitgliedstaat der Europäischen Union betrachtet, in dem die Entscheidungen im Zusammenhang mit den Risikomanagementmaßnahmen vorwiegend getroffen werden. Kann dies nicht eindeutig bestimmt werden oder werden solche Entscheidungen nicht in der Europäischen Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die Risikomanagementmaßnahmen gesetzt werden. Kann dies nicht ermittelt werden, so gilt die Hauptniederlassung als in jenem Mitgliedstaat gelegen, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Europäischen Union hat.

*** Erhält die Cybersicherheitsbehörde von einem anderen Mitgliedstaat der Europäischen Union ein Rechtshilfeersuchen zu einer Einrichtung, die in Österreich „Rechenzentrumsdienste“ anbietet, kann sie innerhalb der Grenzen des Rechtshilfeersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen nach diesem Bundesgesetz in Bezug auf die betreffende Einrichtung ergreifen (siehe § 38 und § 39 NISG 2026 sowie Abschnitt 3.2.3 in diesem Dokument).**

NOTIZ

Die Registrierung hat innerhalb von drei Monaten ab Erfüllung der jeweiligen Voraussetzungen zu erfolgen.

Gemäß der anwendbaren Begriffsbestimmung der NIS-2-RL/NISG2026 wird unter „Einrichtung“ eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person verstanden, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann.

Bei der Registrierung müssen folgende Angaben über einen sicheren Kommunikationskanal strukturiert übermittelt werden:

1. Name der Einrichtung
2. Anschrift und aktuelle Kontaktdaten sowie gegebenenfalls den benannten Vertreter
3. Sektor(en), Teilsektor(en) und Art(en) der Einrichtung
4. Mitgliedsstaaten der Europäischen Union, in denen sie Dienste erbringt
5. Gegebenenfalls die IP-Adressbereiche der Einrichtung
6. Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls sie nicht in der EU niedergelassen ist, die Anschrift ihres benannten Vertreters
7. Informationen zu den im § 25 NISG 2026 angeführten Schwellenwerten betreffend der Unternehmensgröße und ob es sich um eine wesentliche oder wichtige Einrichtung handelt

Gegebenenfalls auftretende Änderungen der Registrierungsangaben müssen der Cybersicherheitsbehörde ehestmöglich, in jedem Fall aber für die Punkte 1 bis 5 innerhalb von zwei Wochen ab dem Tag der Änderung bekanntgegeben werden und für die Punkte 6 bis 7 innerhalb von drei Monaten.

Die Punkte 1 bis 4 und 6 hat die Cybersicherheitsbehörde unter anderem für den Teilsektor „Anbieter von Rechenzentrumsdiensten“ unverzüglich nach deren Erhalt an die Agentur der Europäischen Union für Cybersicherheit (ENISA) weiterzuleiten.

1.3.2 Kriterien für die NISG 2026 Registrierungspflicht im Teilsektor „Rechenzentrumsdienste“

Die NISG 2026 Registrierungspflicht bei der Cybersicherheitsbehörde für betroffene Einrichtungen, die einen „Rechenzentrumsdienst“ erbringen, hängt von folgenden Kriterien ab:

- >> Die betroffene Einrichtung bietet grundsätzlich die qualitativen Kriterien der „Rechenzentrumsdienste“ wie in Abschnitt 1.2 beschrieben an und betreibt und nutzt sie nicht nur ausschließlich für sich selbst.
- >> Unabhängig von der Unternehmensgröße wird die als „Anbieter von Rechenzentrumsdiensten“ agierende betroffene Einrichtung von der Cybersicherheitsbehörde per Bescheid als wesentliche oder wichtige Einrichtung für „Rechenzentrumsdienste“ eingestuft.
- >> Die als „Anbieter von Rechenzentrumsdiensten“ agierende Einrichtung ist ein „großes Unternehmen“ und daher als eine wesentliche Einrichtung einzustufen (beschäftigt zumindest 250 Mitarbeiter oder ein Jahresumsatz von über 50 Millionen Euro und die Jahresbilanzsumme beläuft sich auf über 43 Millionen Euro).
- >> Die als „Anbieter von Rechenzentrumsdiensten“ agierende Einrichtung ist ein „mittleres Unternehmen“ und daher als eine wichtige Einrichtung einzustufen (beschäftigt zumindest 50 Mitarbeiter oder ein Jahresumsatz von über 10 Millionen Euro und die Jahresbilanzsumme beläuft sich auf über 10 Millionen Euro).

Bei der Bestimmung der Anzahl der Mitarbeiter, des Jahresumsatzes und der Jahresbilanzsumme sind die Daten von Partner- oder verbundenen Unternehmen nicht hinzuzurechnen, wenn die Einrichtung in Bezug auf die Netz- und Informationssysteme, die sie bei der Erbringung ihrer Dienste nutzt, sowie unter Berücksichtigung der Beschaffenheit, des Betriebs und der Sicherheit ihrer Netz- und Informationssysteme organisatorisch, technisch und operativ unabhängig von ihren Partner- oder verbundenen Unternehmen ist.

Keine Vererbung der NISG 2026 Pflicht von Kunden/Nutzern (IKT-Betreiber) im Rechneraumbereich des RZ-Standorts.

Die Beurteilung der gesetzlichen NISG 2026 Pflicht ist bezogen auf die Einrichtung, die den „Rechenzentrumsdienst“ wie in Abschnitt 1.2 beschrieben erbringt. Für diese Beurteilung kommt es somit nicht darauf an, ob Kunden/Nutzer (IKT-Betreiber) im Rechnerraumbereich des RZ-Standorts NISG 2026-pflichtig sind oder nicht.

Eine derartige „Vererbung“ ist daher für den Regelfall nach dem Gesetz nicht vorgesehen. Davon unberührt bleibt die freiwillige Übernahme von Verpflichtungen aus der NISG 2026 Sphäre (z. B. Leistungskataloge aus der Durchführungsverordnung) gegenüber seinen Kunden bzw. Vertragspartnern in Verträgen, die jeweils im Einzelfall aus rechtlicher und technischer Sicht geprüft werden sollten.

2 Netz- und Informationssysteme für die Erbringung von Rechenzentrumsdiensten

2.1 Allgemeines zu Netz- und Informationssystemen im NISG 2026 Scope

§32 (1) NISG 2026 beschreibt, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Gemäß der in der NIS-2-RL formulierten Begriffsdefinition (siehe Abschnitt 1.2) umfasst der vom RZ-Betreiber angebotene Dienstleistungsbereich „Rechenzentrumsdienst“ den Betrieb der folgenden zu erbringenden Dienste, welche in der Rechenzentrumsbranche üblicherweise auch als Housing- oder Colocation-Dienstleistung bezeichnet werden (für tiefergehende Erläuterungen siehe dazu Abschnitt 1.3):

- >> Unterbringung (sichere Unterbringung von zentralen IKT-Systemen im Rechnerraum des RZ-Standorts)
- >> Verbindung (der zentralen IKT-Dienste im Rechnerraum des RZ-Standorts mit externen „Kommunikationsdiensten“)
- >> Leistungsverteilung (von elektrischer Energie für die im Rechnerraum untergebrachten IKT-Systeme)
- >> Umgebungskontrolle (Klimatisierung der im Rechnerraum untergebrachten IKT-Systeme)

Im NISG 2026 Scope im Teilsektor „Anbieter von Rechenzentrumsdiensten“ stehen also im Wesentlichen jene Netz- und Informationssysteme, die sich in der Verwaltungshoheit des RZ-Betreibers am RZ-Standort befinden und von den aufgelisteten angebotenen „Rechenzentrumsdiensten“ genutzt werden bzw. diese unterstützen. Darin eingeschlossen sind auch eingebettete Netz- und Informationssysteme bei Geräten der sogenannten RZ-Basisinfrastruktur (siehe Abschnitt 2.2).

Daraus folgt, dass Netz- und Informationssysteme, die im Rechnerraumbereich oder im IKT-Netzverteilbereich des RZ-Standorts untergebracht sind und nicht in der Verwaltungshoheit des „Anbieters von Rechenzentrumsdiensten“ (RZ-Betreiber) stehen, nicht im Scope des Teilsektors „Rechenzentrumsdienste“ stehen – auch wenn sie vielleicht im NISG 2026 Scope eines anderen Teilsektors stehen. Das sind in der Regel jene IKT-Systeme in der Verwaltungshoheit der Kunden des RZ-Betreibers, welche die angebotenen Dienste des „Anbieters von Rechenzentrumsdiensten“ für ihre eigenen Dienste nutzen. Ebenfalls nicht im Scope des Teilsektors „Rechenzentrumsdienst“ steht der Betrieb von öffentlich zugänglichen „Kommunikationsdiensten“ für die Verbindung der IKT-Dienste der Kunden vom RZ-Betreiber mit der Standort-Außenwelt, da diese in einen separaten NISG 2026 Teilsektor fallen und darüber hinaus möglicherweise auch nicht in der Verwaltungshoheit des RZ-Betreibers stehen.

Bietet der „Anbieter von Rechenzentrumsdiensten“ aus dem Rechnerraum an seinem RZ-Standort zusätzlich auch noch andere Dienste aus den Sektoren „Digitale Infrastruktur“ oder „Digitale Dienste“ an, so wäre hier eine gesonderte zusätzliche NISG 2026 Betroffenheit gegeben. Dadurch würde sich dann die NISG 2026 Betroffenheit auch auf die Netz- und Informationssysteme in seiner Verwaltungshoheit erstrecken, die diesen Teilsektoren zuzurechnen sind (z. B. MSP-Dienste oder Cloud-Computing-Dienste, etc.).

Entscheidend für die Zurechnung zum NISG 2026 Scope in einem Sektor bzw. Teilsektor ist immer die Verwaltungshoheit der angebotenen Dienste bzw. der Netz- und Informationssysteme, die diese Dienste nutzen bzw. durch diese unterstützt werden. Es geht darum, welche Einrichtung hat die Befugnis bzw. Hauptverantwortung ein Netz- und Informationssystem:

- >> zu betreiben,
- >> zu konfigurieren,
- >> zu steuern,
- >> zu überwachen
- >> und sicherheitstechnische Maßnahmen umzusetzen.

NOTIZ

Die Verwaltungshoheit ist damit ein Kriterium zur Bestimmung der Verantwortlichkeit im Sinne von NISG 2026.

Die Einrichtung, die die Verwaltungshoheit über die Netz- und Informationssysteme hat, ist auch diejenige, die:

- >> Risikoanalysen durchführen muss,
- >> Sicherheitsmaßnahmen implementieren bzw. die Implementierung veranlassen muss,
- >> Sicherheitsvorfälle melden muss,
- >> und für Verstöße haftet.

Derartige Netz- und Informationssysteme von „Anbietern für Rechenzentrumsdienste“ betreffen vor allem die sogenannte Operational Technology (OT), die für die Erbringung des RZ-Basisinfrastrukturdienstleistungs Bündel herangezogen wird. Zusätzlich können auch „klassische“ IT- und Netzwerksysteme einzubeziehen sein, die der RZ-Betreiber als Zusatzleistungen für seine Kunden anbietet (z. B. Gäste WLAN) oder für eigene administrative Betreibertätigkeiten einsetzt.

2.2 Eingebettete Netz- und Informationssysteme in der physischen RZ-Basisinfrastruktur

Eingebettete Netz und Informationssysteme sind IT- oder besser OT-Systeme, die nicht als eigenständige IKT-Produkte (Computer) erscheinen, sondern fest in technischen Geräten und Anlagen der physischen RZ-Basisinfrastruktur integriert sind. Sie erfüllen digitale Funktionen zur Überwachung und Steuerung der Geräte und Anlagen, sind aber primär Teil eines physischen Systems – oft unauffällig, aber sicherheitskritisch.

NOTIZ

Ein eingebettetes Netz- und Informationssystem ist ein in ein technisches Gerät integriertes digitales System, das:

- >> Daten verarbeitet, speichert oder überträgt,
- >> für die Funktion des Geräts notwendig ist oder dazu beiträgt,
- >> oft über Netzwerk oder Feldbus Schnittstellen kommuniziert,
- >> nicht als klassischer PC oder Server wahrgenommen wird.

Typisch ist, dass Geräte in Anlagen mit eingebetteten Netz- und Informationssystemen eigentlich eine andere Hauptfunktion haben (z. B. für die Energieversorgung und Energieverteilung, die Regelung der Umgebungsbedingungen oder sonstige Funktionen im Bereich der Gebäudetechnik und der Gebäudesicherheit), aber intern digitale Steuerungen nutzen. Derartige Geräte, die in der modernen Gebäudetechnik eingesetzt werden und das schließt auch die im NISG 2026 festgelegten „Rechenzentrumsdienste“ ein, nutzen dabei eine Vielzahl von offenen Standards und Protokollen, um Interoperabilität zwischen verschiedenen Herstellern und Systemen zu gewährleisten. Ethernet und IP-Protokoll spielen dabei eine zentrale Rolle, da es sich als das primäre „Backbone“ für die Kommunikation und Vernetzung durchgesetzt hat. Beispielhaft sind darunter auch weitere Protokolle zu nennen wie SNMP, Modbus, BACnet, KNX, CAN-Bus etc.

Ein angemessenes Maß an Cybersicherheit für die eingebetteten Netz- und Informationssysteme und deren Vernetzung ist erforderlich, da hierüber die Verfügbarkeit (z. B. Abschaltung eines Geräts), Integrität (z. B. Veränderung von Leistungsparametern an einem Gerät) und die Vertraulichkeit (z. B. Preisgabe von Auslastungsinformationen) der Geräte des „Rechenzentrumsdiensts“ kompromittiert werden kann.

Die nachfolgende Tabelle gibt einen beispielhaften Überblick für Geräte und Systeme mit eingebetteten Netz- und Informationssystemen, welche über die im NISG 2026 festgelegten „Rechenzentrumsdienste“ genutzt werden bzw. diese Dienste unterstützen:

„Rechenzentrumsdienst“ gemäß Definition NISG 2026:	Beispiele für Geräte in Anlagen mit eingebetteten Netz- und Informationssystemen:	
Housing / Colocation (<u>Zentrale Unterbringung</u> von IT- und Netzausrüstung)	>> Brandmeldeanlagen und Brandbekämpfungsanlagen >> Einbruchmeldeanlagen >> Gebäudeleittechnik	>> Elektronische Zutrittskontrollanlagen >> Videoüberwachung >> Sicherheitsleitstand
Energieversorgung und Energieverteilung (Anlagen und Infrastrukturen für die <u>Leistungsverteilung</u>)	>> Unterbrechungsfreie Strom-versorgungen (USV) >> Netzersatzanlagen (NEA)	>> Lastschalter, Lasttrenner >> Power Distribution Units (PDU)
Geregelte Umgebungsbedingungen / Klimatisierung (Anlagen und Infrastrukturen für die <u>Umgebungskontrolle</u>)	>> Kältemaschinen und Kälteanlagen >> Rückkühleinheiten	>> Pumpen in der Kälteverteilung >> Umluftkühler (ULK)

Tabelle 1: Rechenzentrumsdienste und Beispiele für Geräte und Anlagen mit eingebetteten Netz- und Informationssystemen

Im Scope des NISG 2026 stehen in Geräten eingebettete Netz- und Informationssysteme im Teilsektor „Anbieter von Rechenzentrumsdiensten“, wenn sie:

- >> für die Erbringung eines Rechenzentrumsdienstes notwendig sind oder diesen unterstützen,
- >> über Netzwerk erreichbar sind,
- >> oder bei einer Kompromittierung die Verfügbarkeit, Integrität oder Vertraulichkeit des Rechenzentrumdienstes gefährden.

3 Anforderung für Risikomanagementmaßnahmen im Bereich der Cybersicherheit

3.1 Risikomanagementmaßnahmen gemäß § 32 NISG 2026

Betroffene wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen (Umfang und Definition der Rechenzentrumsdienste siehe Abschnitt 2), zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste, sprich: auf die Kunden des „Anbieters von Rechenzentrumsdiensten“ und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die **Risikomanagementmaßnahmen** haben zudem unter **Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen** sowie bewährter Verfahren und der Kosten der Umsetzung ein Cybersicherheitsniveau zu gewährleisten, das dem bestehenden Risiko angemessen ist.

Bei der Beurteilung der Verhältnismäßigkeit der Risikomanagementmaßnahmen sind das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

Diese Risikomanagementmaßnahmen haben auf einem gefahrenübergreifenden Ansatz zu beruhen, der auf den Schutz der Netz- und Informationssysteme samt deren physischen Komponenten (siehe dazu auch Abschnitt 2.2) vor Cybersicherheitsvorfällen abzielt, und zumindest folgende Inhalte zu umfassen:

- a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- b) Bewältigung von Cybersicherheitsvorfällen
- c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern, unter Berücksichtigung der spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, der Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, sowie der Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen
- e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
- j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Die Cybersicherheitsbehörde ist ermächtigt, durch Verordnung nähere Anforderungen an die Risikomanagementmaßnahmen festzulegen. Dabei kann die Cybersicherheitsbehörde insbesondere anordnen, dass die von der Europäischen Kommission auf Grundlage des Art. 21 Abs. 5 der NIS-2-Richtlinie erlassenen Durchführungsrechtsakte* zur Festlegung technischer und methodischer Anforderungen an Risikomanagementmaßnahmen auch auf andere Sektoren oder Arten von Einrichtungen Anwendung finden. Dies gilt auch dann, wenn die Durchführungsrechtsakte ursprünglich nur für einzelne Sektoren oder bestimmte Arten von Einrichtungen erlassen wurden, sektorspezifische Besonderheiten können dabei berücksichtigt werden.



***Anwendung der Durchführungsverordnung (EU) 2024/2690 für „Anbieter von Rechenzentrumsdiensten“:**

Im § 27 (1) NISG 2026 ist festgehalten, dass die weiter oben dargelegten Anforderungen für Risikomanagementmaßnahmen aus dem § 32 NISG 2026 insoweit nicht anwendbar sind, als wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer unionsrechtlicher Bestimmungen zur Ergreifung von Risikomanagementmaßnahmen verpflichtet sind und die jeweiligen Bestimmungen dieser sektorspezifischen Rechtsakte ein zumindest gleichwertiges Cybersicherheitsniveau gewährleisten.

Die Durchführungsverordnung (EU) 2024/2690 beinhaltet mit unmittelbarer Wirksamkeit derartige sektorspezifische unionsrechtliche Bestimmungen, insbesondere im Artikel 2 und in deren Anhang, wo in 13 Hauptabschnitten technische und methodische Anforderungen unter anderem für den Teilsektor „Anbieter von Rechenzentrumsdiensten“ festgelegt sind.

3.2 Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

3.2.1 Selbstdeklaration

Wesentliche und wichtige Einrichtungen – darunter auch betroffene Einrichtungen, die „Anbieter von Rechenzentrumsdiensten“ sind – haben innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht (welche für betroffenen Einrichtungen erstmalig ab dem 1.10.2026 beginnt) der Cybersicherheitsbehörde Informationen hinsichtlich der umgesetzten Risikomanagementmaßnahmen nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form als Selbstdeklaration zu übermitteln. Dazu zählen insbesondere die genutzten Netz- und Informationssysteme (siehe Abschnitt 2) und die Sicherheit der Lieferketten sowie die Ergebnisse der durchgeführten Risikoanalyse (siehe NISG 2026 § 33 (1)).

Es ist für „Anbieter von Rechenzentrumsdiensten“ davon auszugehen, dass bei der Selbstdeklaration auch die an den betreffenden RZ-Standorten jeweils realisierte und den Kunden an diesen Standorten angebotene Verfügbarkeitsklasse des Rechenzentrumsdienstleistungs-bündel (siehe Abschnitt 1.2.2) anzugeben ist. Dies ist ein wesentliches Kriterium für die im Zuge einer Prüfung zu beurteilende angemessene Umsetzung der Risikomanagementmaßnahmen im Bereich der laut der Durchführungsverordnung (EU) 2024/2690 betitelten „unterstützenden Versorgungsleistungen“. Ohne Angabe der angebotenen Verfügbarkeitsklasse, im Rahmen der vier möglichen Optionen aus der diesbezüglich einschlägigen europäischen Norm EN 50600, fehlt ansonsten die Beurteilungsgrundlage für die Angemessenheit.

¹ Siehe Durchführungsverordnung (EU) 2024/2690, Anhang, Abschnitt 13.1.2 „...müssen die betreffenden Einrichtungen – soweit angemessen – ...b) die Nutzung von Redundanzsystemen für Versorgungsleistungen in Erwägung ziehen“.

Bei der Übermittlung der Informationen hinsichtlich der umgesetzten Risikomanagementmaßnahmen ist es empfehlenswert, auf die Berücksichtigung des Standes der Technik zu referenzieren bzw. diesen nachzuweisen. Ausgestellte einschlägige Zertifikate von anerkannten (akkreditierten) Zertifizierungsstellen bieten hier eine gute Plausibilitätsgrundlage. Folgende akkreditierte Zertifizierungen können für „Anbieter von Rechenzentrumsdienstleistungen“ jedenfalls als einschlägig angesehen werden:

- >> Zertifizierung nach ISO/IEC 27001 „Informations-Sicherheits-Management-Systeme“ (deckt insbesondere das Management der Informationssicherheit für den Bereich der Netz- und Informationssysteme ab)
- >> Zertifizierung nach EN 50600 „Einrichtungen und Infrastrukturen von Rechenzentren“ (deckt den Bereich der unterstützenden Einrichtungen (Energieversorgung und -verteilung sowie Regelung der Umgebungsbedingungen sowie die physische Sicherheit der Netz- und Informationssysteme und der unterstützenden Einrichtungen an RZ-Standorten ab)

3.2.2 Prüfung durch unabhängige Stelle

Wesentliche und wichtige Einrichtungen – darunter auch betroffene Einrichtungen, die „Anbieter von Rechenzentrumsdiensten“ sind – haben innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde die technische, operative und organisatorische Umsetzung der Risikomanagementmaßnahmen nachzuweisen. Dies hat durch eine von einer „unabhängigen Stelle“ (die von der Cybersicherheitsbehörde zugelassen ist) durchgeführten Prüfung, die nicht länger als zwei Jahre zurückliegt, zu geschehen.

Die Prüfung hat nach den Vorgaben der Cybersicherheitsbehörde sowie auf Basis der von der jeweiligen Einrichtung durchgeführten Risikoanalyse zu erfolgen oder aufgrund sonstiger Risikoabwägungen.

Der Nachweis der operativen sowie organisatorischen Umsetzung der Risikomanagementmaßnahmen ist auch durch einschlägige Zertifikate möglich.

Davon abweichend haben wesentliche Einrichtungen die operative sowie organisatorische Umsetzung der Risikomanagementmaßnahmen innerhalb von zwei Monaten nach Aufforderung durch die Cybersicherheitsbehörde nachzuweisen.

Die erstmalige Aufforderung kann frühestens nach Ablauf von zwei Jahren ab Inkrafttreten des NISG 2026 (1.10.2026) erfolgen.

Für alle Sektoren und Teilsektoren können aus jetziger Sicht ausgestellte Zertifikate von akkreditierten Zertifizierungsstellen für folgende akkreditierten Zertifizierungen als einschlägige Zertifikate angesehen werden:

- >> Zertifizierung nach ISO/IEC 27001 „Informations-Sicherheits-Management-Systeme“ (deckt insbesondere das Management der Informationssicherheit für den Bereich der Netz- und Informationssysteme ab)

Zusätzlich können für den Teilsektor „Anbieter für Rechenzentrumsdienste“ ausgestellte Zertifikate von akkreditierten Zertifizierungsstellen für folgende Zertifizierungen als einschlägige Zertifikate angesehen werden:

- >> Zertifizierung nach EN 50600 „Einrichtungen und Infrastrukturen von Rechenzentren“ (deckt den Bereich der unterstützenden Einrichtungen (Energieversorgung und -verteilung sowie Regelung der Umgebungsbedingungen sowie die physische Sicherheit der Netz- und Informationssysteme und der unterstützenden Einrichtungen an RZ-Standorten ab)

3.2.3 Anlassbezogene Kontrollen durch die Cybersicherheitsbehörde

Die Cybersicherheitsbehörde ist in Wahrnehmung ihrer Aufsichtsaufgaben zur Einhaltung des sich aus dem NISG 2026 ergebenden Verpflichtungen in Bezug auf wesentliche Einrichtungen befugt, folgende Maßnahmen zu ergreifen:

1. Durchführung von Kontrollen der Umsetzung der Risikomanagementmaßnahmen gemäß § 32 NISG 2026 durch Einschau, insbesondere in die diesbezüglichen Netz- und Informationssysteme und Unterlagen vor Ort und aus der Ferne unter Mitwirkung der Einrichtung oder durch Begleitung der Prüfungen durch unabhängige Stellen, jeweils nach vorangegangener Verständigung der betreffenden Einrichtung.
2. Durchführung von Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung.
3. Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung umgesetzten Risikomanagementmaßnahmen gemäß § 32 NISG 2026 erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung der Informationen gemäß § 29 NISG 2026 für die Registrierung.
4. Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind.
5. Ad-hoc-Prüfung einer wesentlichen Einrichtung, einschließlich solcher, die aufgrund eines erheblichen Cybersicherheitsvorfalls oder Verstoßes gegen das NISG 2026 durch diese Einrichtung gerechtfertigt sind oder der Überprüfung einer übermittelten Selbstdeklaration gemäß § 33 (1) NISG 2026 dienen.

Erlangt die Cybersicherheitsbehörde durch Nachweise, wie insbesondere die Selbstdeklaration gemäß § 33 (1) NISG 2026, oder sonstige begründete Hinweise und Informationen davon Kenntnis, dass eine wichtige Einrichtung mutmaßlich ihren Verpflichtungen nach dem NISG 2026, insbesondere der Umsetzung von Risikomanagementmaßnahmen gemäß § 32 NISG 2026 und den Berichtspflichten gemäß § 34 NISG 2026, nicht nachkommt, kann sie auch gegenüber wichtigen Einrichtungen die weiter oben angeführten Aufsichtsmaßnahmen Punkt 1 bis 4 setzen.

Die Ausübung der Aufsichtsmaßnahmen hat in dem unbedingt erforderlichen Ausmaß sowie unter möglicher Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs zu erfolgen.

4 Ausblick auf die Weiterentwicklung dieses Positionspapiers

Im Zuge der Weiterentwicklung dieses ADCA Positionspapiers ist angedacht, in weiteren Ausgaben (Versionen) auch die folgenden Themenbereiche näher zu beleuchten:

- >> Stand der Technik und einschlägige Normen für „Rechenzentrumsdienste“
- >> Risikomanagementmaßnahmen gemäß Durchführungsverordnung (EU) 2024/2690
- >> Ansätze für die Umsetzung von geforderten Risikomanagementmaßnahmen
- >> Meldung von erheblichen Sicherheitsvorfällen im Teilsektor „Anbieter von Rechenzentrumsdiensten“
- >> Exkurs zu RKEG (Resilienz kritischer Einrichtungen-Gesetz) Anforderungen

Bei der Herausgabe eines neuen Ausgabestands werden, entsprechend dem aktuellen Stand neuer Erkenntnisse, natürlich auch die bereits ausgearbeiteten Abschnitte überarbeitet.

Auf ein Date mit der Austrian Data Center Association

Sie haben Fragen oder wollen mehr über uns erfahren?
Dann treten Sie mit uns in direkten Kontakt:



Austrian Datacenter Association
Verein Österreichischer Rechenzentrumsbetreiber
Rockhgasse 6, Top 6, 1010 Wien
office@austriandatacenter.org
austriandatacenter.org

