# NIS - Verpflichtungen für Anbieter digitaler Dienste im Bereich Netz- und Informationssystemsicherheit (EU-NIS-RL, EU-NIS-Df-VO, NISG, NISV)

## EU-NIS-Richtlinie, NIS-Gesetz und NIS-Verordnung

Die EU-Richtlinie (2016/1148) über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU (EU-NIS-RL) wurde in Österreich durch das Netz- und Informationssystemsicherheitsgesetz (NISG), auf dessen Grundlage auch eine entsprechende Verordnung (NISV) erlassen wurde, umgesetzt. Darüber hinaus existiert auf EU-Ebene für diesen Bereich noch die Durchführungsverordnung (EU) 2018/151 (EU-NIS-Df-VO).

Mit diesen Regelungen für den Bereich Cybersicherheit wird das Ziel verfolgt, ein hohes Sicherheitsniveau der Netz- und Informationssicherheitssysteme sicherzustellen. Neben Festlegungen von Aufgaben und Behördenstrukturen, Vorgaben für die Einrichtung und Koordination zur Prävention und Bewältigung von IT-Sicherheitsvorfällen sowie von Computer-Notfallteams zur Unterstützung der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung bei der Bewältigung von IT-Risiken, Vorfällen und Sicherheitsvorfällen werden konkrete rechtliche Vorgaben auch für bestimmte Unternehmen dahingehend gemacht, passende IT-Sicherheitsmaßnahmen einzuführen und darüber hinaus schwerwiegende IT-Störfälle zu melden.

## Anbieter digitaler Dienste - von Gesetzes wegen zur Einhaltung des NISG verpflichtet

Während die Ermittlung sog Betreiber wesentlicher Dienste (z.B. bestimmte Dienste in den Bereichen Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung & -versorgung und digitale Infrastruktur) auf hoheitlichem Wege erfolgt und die entsprechend ermittelten Unternehmen mittels Bescheid über die Einbeziehung in die entsprechenden Verpflichtungen verständigt werden, bestehen für sog **Anbieter digitaler Dienste** bestimmte Verpflichtungen im Zusammenhang mit Netz- und Informationssystemsicherheit bereits von Gesetzes wegen. Eine Ermittlung auf hoheitlichem Wege samt Bestimmung mittels Bescheid ist für diese Gruppe von Unternehmen nicht vorgesehen. Betroffene Unternehmen haben die rechtlichen Vorgaben in diesem Bereich vielmehr zu erfüllen, ohne dazu aufgefordert worden zu sein.

## Was ist ein digitaler Dienst gemäß NISG?

Ein digitaler Dienst nach dem NISG ist ein Dienst der Informationsgesellschaft, dh ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst, bei dem es sich um

- einen **Online-Marktplatz**,
- eine **Online-Suchmaschine** oder
- einen **Cloud-Computing-Dienst** handelt.

## Wer gilt als Anbieter digitaler Dienste?

Anbieter digitaler Dienste sind juristische Personen oder eingetragene Personengesellschaften, die einen digitalen Dienst in Österreich anbieten und eine Hauptniederlassung in Österreich haben oder einen Vertreter in Österreich namhaft gemacht haben.

Anbieter digitaler Dienste ohne Hauptniederlassung in der Europäischen Union sind verpflichtet, einen **Vertreter** in einem Mitgliedstaat namhaft zu machen. Dieser Vertreter handelt im Auftrag des digitalen Diensteanbieters und ist die Kontaktstelle für die zuständigen Stellen in den Mitgliedstaaten.

## Wer gilt nicht als Anbieter digitaler Dienste?

- Ausdrücklich **nicht** als **Anbieter digitaler Dienste** gelten natürliche Personen, Kleinstunternehmen und kleine Unternehmen, dh Unternehmen mit weniger als 50 Mitarbeitern

**und**

- einem Jahresumsatz bzw. einer Jahresbilanz von unter EUR 10 Mio.

## Was ist ein Online-Marktplatz im Sinne des NISG?

Ein Online-Marktplatz im Sinne des NISG ermöglicht es Verbrauchern und Unternehmern, Kaufverträge oder Dienstleistungsverträge mit Unternehmern online abzuschließen und ist als solcher der endgültige Bestimmungsort für den Abschluss dieser Verträge.

**Nicht** erfasst sind Online-Dienste, die lediglich als Vermittler für Drittdienste fungieren und durch die letztlich ein Vertrag geschlossen werden kann. **Ebenso wenig** erfasst sind Online-Dienste, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft.

Die von einem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschließen. Als Online-Stores tätige Application-Stores, die den digitalen Vertrieb von Anwendungen oder Software-Programmen von Dritten ermöglichen, sind Online-Marktplätze im weiteren Sinn.

## Was ist eine Online-Suchmaschine im Sinne des NISG?

Eine Online-Suchmaschine ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Websites anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Websites in einer bestimmten Sprache beschränkt sein.

Die Definition des Begriffs „Online-Suchmaschine" erstreckt sich **nicht** auf Suchfunktionen, die auf den Inhalt einer bestimmten Website beschränkt sind (z.B. Kontextsuche oä), unabhängig davon, ob die Suchfunktion durch eine externe Suchmaschine bereitgestellt wird.

Sie erstreckt sich auch **nicht** auf Online-Dienste, die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten (z.B. Preisvergleichsplattformen).

## Was sind Cloud Computing Dienste im Sinne des NISG?

Cloud Computing Dienste umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Für die Zwecke der NIS-Richtlinie und des NISG sind unter dem Begriff „Cloud Computing Dienste" Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste.

Der Begriff „skalierbar" bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool" wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können.

Der Begriff „gemeinsam nutzbar" wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird.

## Werden Anbieter digitaler Dienste ermittelt?

Nein. Anbieter digitaler Dienste müssen sich nach dem NIS-Gesetz selbst identifizieren.

## Welche Pflichten haben Anbieter digitaler Dienste?

Anbieter digitaler Dienste haben in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, (**präventiv**) geeignete und verhältnismäßige technische und organisatorische **Sicherheitsvorkehrungen** zu treffen. Nähere Informationen und Hilfestellungen hiezu sind in den Empfehlungen bzw. Guidance Documents der ENISA enthalten (https://www.enisa.europa.eu). Diese Sicherheitsvorkehrungen haben unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden mit vernünftigem Aufwand feststellbaren Risiko angemessen ist, wobei Folgendem Rechnung zu tragen ist:

a. Sicherheit der Systeme und Anlagen,
b. Bewältigung von Sicherheitsvorfällen,
c. Betriebskontinuitätsmanagement,
d. Überwachung, Überprüfung und Erprobung,

e. Einhaltung der internationalen Normen.

Die Elemente, die von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden sind, werden in der Durchführungsverordnung (EU) 2018/151 festgelegt.

Anbieter digitaler Dienste haben einen **Sicherheitsvorfall (**= eine Störung von erheblicher Auswirkung, zu diesem Begriff im Einzelnen unten**)**, der einen digitalen Dienst betrifft, unverzüglich zu melden (**reaktiv**).

Zuständig für die Entgegennahme der Meldung von Anbietern digitaler Dienste ist das nationale Computer-Notfallteam. In Österreich ist dies das Computer Emergency Response Team Austria (**CERT.at**).

Die Meldung wird vom nationalen Computer-Notfallteam an den Bundesminister für Inneres weitergeleitet.

Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls zu bewerten.

## Wann liegt ein Sicherheitsvorfall vor?

Ein **Sicherheitsvorfall**, der als solcher beim Anbieter eine Meldepflicht auslöst, liegt dann vor, wenn eine **Störung** der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen digitalen Dienstes **von erheblicher Auswirkung** geführt hat.

Ein Sicherheitsvorfall kann neben Cyberangriffen oder Einwirkungen Dritter auch durch physische Ereignisse wie etwa Naturereignisse, aber auch durch Ereignisse wie z.B. Stromausfälle oder das Verhalten eigener Mitarbeiter verursacht werden.

## Wann gelten die Auswirkungen einer Störung als erheblich?

Bei der Beurteilung, ob eine Störung **erhebliche Auswirkungen** hat und somit einen **Sicherheitsvorfall** darstellt, sind insbesondere die Anzahl der betroffenen Nutzer, die Dauer der Störung, die geografische Ausbreitung der Störung sowie die Auswirkung auf wirtschaftliche oder gesellschaftliche Tätigkeiten zu berücksichtigen.

Im Falle von Anbietern digitaler Dienste sind die Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls in der EU-NIS-Df-VO festgelegt.

Ein Sicherheitsvorfall gilt als mit erheblichen Auswirkungen verbunden, wenn **mindestens einer** der folgenden Fälle eingetreten ist:

- Der von einem Anbieter digitaler Dienste bereitgestellte Dienst war **mehr als 5.000.000 Nutzerstunden** (Zahl der Nutzer **in Union**, die während einer Dauer von **sechzig Minuten** betroffen waren) lang **nicht verfügbar;** oder
- der Sicherheitsvorfall hat zu einem **Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten** oder entsprechender Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden bzw. zugänglich sind, geführt, von dem **mehr als 100.000 Nutzer in der Union betroffen** sind; oder
- durch den Sicherheitsvorfall ist eine öffentliche **Gefahr oder ein Risiko für die öffentliche Sicherheit** entstanden **oder** es sind **Menschen ums Leben gekommen;** oder
- der Sicherheitsvorfall hat **für mindestens einen Nutzer in der Union** zu einem **Sachschaden in Höhe von mehr als EUR 1.000.000** geführt.

## Wie sieht ein Meldevorgang für Anbieter digitaler Dienste aus?

Anbieter digitaler Dienste haben einen Sicherheitsvorfall, der einen von ihnen bereitgestellten digitalen Dienst betrifft, unverzüglich an das nationale Computer-Notfallteam (CERT.at) zu melden. Dieses leitet die Meldung in weiterer Folge unverzüglich an den Bundesminister für Inneres weiter.

## Welche Inhalte muss die Meldung eines Sicherheitsvorfalles aufweisen?

Die Meldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und den technischen Rahmenbedingungen, die zum Zeitpunkt der Erstmeldung bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in Nachmeldungen und letztendlich in einer Abschlussmeldung ohne unangemessene weitere Verzögerung mitzuteilen. Die Meldung ist in einem standardisierten elektronischen Format (siehe näher Button „Pflichtmeldung Anbieter digitaler Dienste“ unter https://nis.cert.at/) zu übermitteln.

## Welches Computer-Notfallteam ist für die Entgegennahme von Meldungen für Anbieter digitaler Dienste zuständig?

Das für die Entgegennahme von Meldungen durch Unternehmen zuständige Computer-Notfallteam ist das nationale Computer-Notfallteam, in Österreich das

CERT.at - Computer Emergency Response Team Austria

Webseite: www.cert.at

Telefon: +43 1 5056416 78

Verpflichtende und freiwillige NIS-Meldungen: https://nis.cert.at

E-Mail-Adresse für sonstige Meldungen: reports@cert.at

E-Mail-Adresse für andere Anfragen: team@cert.at

## Was sind Computer-Notfallteams?

Computer Notfallteams bzw. CSIRTs – Computer Security Incident Response Teams (auch: CERTs – Computer Emergency Response Teams) sind für die Prävention, Erkennung, Reaktion und Folgenminderung bei Risiken, Vorfällen und Sicherheitsvorfällen wichtig. Durch das NIS-Gesetz werden zur Gewährleistung der Sicherheit von Netz- und Informationssystemen Computer-Notfallteams eingerichtet.

## Was ist eine freiwillige Meldung?

Anbietern digitaler Dienste wird durch das NISG - ebenso wie Betreibern wesentlicher Dienste und Einrichtungen der öffentlichen Verwaltung - die Möglichkeit eingeräumt, Risiken und Vorfälle freiwillig an das zuständige Computer-Notfallteam zu melden. Der Meldeweg unterscheidet sich grundsätzlich nicht von jenem für eine verpflichtende Meldung, jedoch können freiwillige Meldungen auch zeitverzögert, aggregiert und ohne namentliche Nennung der Melder an das Bundesministerium für Inneres weitergeleitet werden.

## Was sind nationale zuständige Behörden gemäß NIS-Richtlinie?

Jeder Mitgliedstaat hat gemäß NIS-Richtlinie eine oder mehrere für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde zu benennen. Diese werden als „zuständige Behörde" bezeichnet. Ihre Aufgabe ist die Überwachung der Anwendung der NIS-Richtlinie auf nationaler Ebene. In Österreich sind dies das **Bundeskanzleramt und** das **Bundesministerium für Inneres**.

## Wird die Umsetzung der Verpflichtungen überprüft?

Anbieter digitaler Dienste unterliegen (im Vergleich zu Betreibern wesentlicher Dienste) weniger strikten, **präventiven Bereithaltungspflichten** für Sicherheitsvorkehrungen und **reaktiven Aufsichtstätigkeiten**, die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind.

Der Bundesminister für Inneres ist, wenn ihm nachweisliche Umstände bekannt werden, dass ein Anbieter digitaler Dienste den Anforderungen aus dem NIS-Gesetz nicht nachkommt, ermächtigt zu verlangen, dass dieser **Nachweise** über geeignete **Sicherheitsvorkehrungen** (präventive Maßnahmen) erbringt.

Der Bundesminister für Inneres kann dazu Einschau in die Netz- und Informationssysteme, die für die Bereitstellung des digitalen Dienstes genutzt werden, und diesbezügliche Unterlagen nehmen.

## Welche Strafen sind bei Verstößen möglich?

Ein Verstoß gegen die Vorgaben des NISG (gegen Meldepflicht, Sicherheitsvorkehrungen, Mitwirkungspflichten) wird mit einer Geldstrafe von bis zu EUR 50.000 sanktioniert, im Wiederholungsfall bis zu EUR 100.000. Zuständig für die Sanktionen sind die Bezirksverwaltungsbehörden. Die Bezirksverwaltungsbehörden können Geldstrafen auch gegen juristische Personen verhängen.

## Weiterführende Informationen

Weiterführende Informationen zum Thema Netz- und Informationssystemsicherheit (einschließlich Kontaktdaten von Behörden) sind auf der vom Bundeskanzleramt und dem Bundesministerium für Inneres betriebenen Website www.nis.gv.at verfügbar.

Stand: 27.01.2021