LEITFADEN

DIE NIS2-RICHTLINIE

RELEVANZ FÜR DEN HANDEL

HANDELS VERBAND

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

1. WORUM HANDELT ES SICH BEI DER NIS2-RICHTLINIE?

ALLGEMEINES

Bei der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (kurz: „NIS2-RL“) handelt es sich um die Nachfolgeregelung der ersten Cybersicherheits-Richtlinie der Europäischen Union („NIS-RL“), welche in Österreich im Netz- und Informationssystemsicherheitsgesetz (kurz: „NISG“) umgesetzt wurde.

Bereits durch die erste NIS-RL und deren nationale Umsetzung im NISG wurden bestimmte Unternehmen zu Cybersicherheits-Maßnahmen verpflichtet. Mit der Nachfolgeregelung, der NIS2-RL, wird der Anwendungsbereich signifikant erweitert, um auch große Teile bisher nicht erfasster Unternehmen zu bedarfsgerechten Sicherheitsmaßnahmen zu verpflichten. Darüber hinaus werden insbesondere konkrete Vorgaben für ein Meldesystem bei Sicherheitsvorfällen gemacht und neue Haftungstatbestände geschaffen. Auch soll die Zusammenarbeit zwischen den diversen nationalstaatlichen Behörden untereinander verbessert und klarer strukturiert werden.

BACKGROUND INFO

Das derzeit geltende NISG wird durch die nationale NIS-Verordnung („NISV“) ergänzt, welche spezifischere Vorgaben beinhaltet. Darüber hinaus existieren sogenannte NIS-Factsheets mit umfangreichen Informationen zur derzeitigen Rechtslage.

Österreich hat bis zum 17. Oktober 2024 Zeit, die NIS2-RL in nationales Recht umzusetzen. Im Zuge dessen wird auch eine entsprechende Anpassung des NISG und der NISV vom nationalen Gesetzgeber vorzunehmen sein.

PRAXISTIPP

Selbst wenn die NIS2-RL noch nicht umgesetzt ist, empfiehlt es sich bereits frühzeitig abzuklären, ob das eigene Unternehmen von dieser erfasst ist. Allfällige Vorlaufzeiten zur Herstellung des geforderten Zustands sollten möglichst berücksichtigt werden.

HANDELS VERBAND STADLER VÖLKEL RECHTSANWÄLTE · ATTORNEYS AT LAW

2. BIN ICH ALS HÄNDLER*IN VON DER NIS2-RL BETROFFEN?

ALLGEMEINES

Die jeweils zu überschreitende Schwelle für eine Anwendbarkeit der NIS2-RL ist niedrig. Dies führt – im Gegensatz zur ersten NIS-RL – zu einem weitaus umfangreicheren Anwendungsbereich.

Damit Händler*innen von deren Vorgaben erfasst werden, müssen grundsätzlich gewisse Größen- bzw. Typkriterien erfüllt sein. Kleine Unternehmen sind von der Richtlinie prinzipiell ausgenommen. Darüber hinaus existieren verschiedene weitere Ausnahmeregelungen.

Die NIS2-RL gilt allerdings nicht für jedes Unternehmen:

NACH GRÖSSE

Allgemeine Anforderung: Die Tätigkeitsausübung oder Diensteerbringung findet innerhalb der EU statt und die Tätigkeit fällt unter Anhang I oder II der NIS2-RL (siehe relevante Sektoren unten).

Zumindest mittelgroßes Unternehmen: ab 50 Mitarbeiter*innen ODER mehr als 10 Mio. Euro Jahresumsatz.

UNABHÄNGIG VON DER GRÖSSE

... für Einrichtungen der in Anhang I oder II genannten Sektoren, wenn

- es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;
- sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;
- eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzüberschreitende Auswirkungen haben könnte;
- die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist;

... für Einrichtungen, welche nach der Richtlinie für Resilienz kritischer Einrichtungen (CER-Richtlinie) als kritisch eingestuft wurden.

BACKGROUND INFO

In den erwähnten Anhängen der NIS2-RL sind insbesondere folgende für den Handel relevante Sektoren bzw. Einrichtungen genannt:

Trinkwasser, Post- und Kurierdienste, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Anbieter von Online-Marktplätzen.

PRAXISTIPP

Die Berechnung der Größenschwellen nach der relevanten Empfehlung 2003/361/EG ist komplex, da dafür auch auf mittelbare Zurechnungen und vertragliche Aspekte abgestellt wird (z. B. verbundene Unternehmen oder Tochtergesellschaften). Gerade bei größeren Konzernen sind diesfalls Einzelfallprüfungen sinnvoll.

Für die Berechnung der Größenschwellen wurde von der Europäischen Kommission eine umfangreiche Anleitung veröffentlicht (https://op.europa.eu/s/y3fM). Es empfiehlt sich allerdings trotzdem, professionelle rechtliche Beratung zur Bewertung der Frage der Anwendbarkeit der NIS2-RL in Anspruch zu nehmen – vor allem bei komplexeren Unternehmensstrukturen.

3. SIND AUCH KLEINE UNTERNEHMEN ERFASST?

Kleine Unternehmen, also solche, die weniger als 50 Mitarbeiter*innen beschäftigen und einen Jahresumsatz von höchstens 10 Mio. Euro erzielen, sind von der Richtlinie – unbeschadet einer Einbeziehung aus größenunabhängigen Kriterien – grundsätzlich ausgenommen.

Zu einer mittelbaren Verpflichtung von kleinen Unternehmen kann es aber insbesondere im Bereich der Lieferketten kommen, wenn kleine Unternehmen über vertragliche Konstruktionen zur Einhaltung der NIS2-RL verpflichtet werden.

Das heißt auch Dienstleister*innen und Lieferant*innen von betroffenen Unternehmen müssen Sicherheitsvorkehrungen einhalten.

4. WELCHE SPEZIFISCHEN VERPFLICHTUNGEN KOMMEN AUF ERFASSTE UNTERNEHMEN ZU?

ALLGEMEINES

Die NIS2-RL sieht insbesondere eine Verpflichtung zur Setzung von Governance- & Risikomanagement-Maßnahmen vor.

Wie sich unten bei den Governance- und Risikomanagement-Maßnahmen noch konkret zeigen wird, verfolgt die NIS2-RL einen sogenannten „all hazards approach“. Dies bedeutet, dass die NIS2-RL nicht bloß Maßnahmen zum Schutz vor Cyber-Bedrohungen vorsieht, sondern vor jeglichen Gefahren tatsächlicher oder potentieller Natur in diesem Kontext. So sind beispielsweise auch Vorgaben zum Schutz vor Naturkatastrophen, Einbruch, Feuer oder aber auch Stromausfällen mitumfasst.

BACKGROUND INFO

Die genannten Verpflichtungen stellen den Mittelpunkt der NIS2-RL für Unternehmen dar. Insbesondere die Notwendigkeit, an Schulungen zur Cybersicherheit teilzunehmen und diese anzubieten, spiegelt die herausragende Bedeutung des Faktors Mensch wider. Oftmals stellt dieser ein nicht zu unterschätzendes Risiko für Verfehlungen dar.

PRAXISTIPP

Es empfiehlt sich, hier jedenfalls den IST-Zustand und allfällige Unterschiede zum SOLL-Zustand zu erheben. Entsprechende Anpassungen bedürfen oft gewisser Vorlaufzeiten.

HANDELS VERBAND STADLER VÖLKEL RECHTSANWÄLTE · ATTORNEYS AT LAW

5. WELCHE RISIKOMANAGEMENT-MASSNAHMEN SIND EINZUHALTEN?

ALLGEMEINES

Einer der Kernpunkte der NIS-2 RL betrifft Risikomanagement-Maßnahmen im Bereich der Cybersicherheit.

Der EU-Gesetzgeber hat Österreich dazu verpflichtet sicherzustellen, dass jedenfalls wesentliche und wichtige Einrichtungen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ ergreifen müssen, um gewisse Cyberrisiken hintanzuhalten.

Bei den jeweiligen Risikomanagement-Maßnahmen muss im Sinne eines risikobasierten Ansatzes (also „Verhältnismäßigkeit“) auf den Stand der Technik, auf die Kosten für die Einrichtung sowie auf weitere individuelle Faktoren (Einrichtungsgröße, Wahrscheinlichkeit eines Sicherheitsrisikos usw.) Rücksicht genommen werden.

Art 21 Abs. 2 lit a–j der Richtlinie zählt dabei 10 Maßnahmen und Mindeststandards auf, die in jedem Fall eingehalten werden müssen. Diese umfassen:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Maßnahmen zur Bewältigung von Sicherheitsvorfällen;
- Maßnahmen zur Aufrechterhaltung des Betriebs;
- Maßnahmen betreffend die Sicherheit der Lieferkette;
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von Netz- und Informationssystemen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-Maßnahmen
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulung;
- Konzepte und Verfahren i. Z. m. Kryptografie/Verschlüsselungen;
- Sicherheit des Personals, Konzepte für Zugriffskontrolle/Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung sowie gesicherte Kommunikationsmittel.

BACKGROUND INFO

Neben der nationalen Umsetzung sind auch bestimmte von der EU-Kommission zu erlassende technische und methodische Spezifikationen zu beachten. Diesen Durchführungsrechtsakten wird große Bedeutung beizumessen sein.

PRAXISTIPP

Zur Einhaltung des Risikomanagements wird auch auf ISO-Normen (z. B. ISO-27000) verwiesen.

Zu den Risikomanagement-Maßnahmen, zu welchen auch geeignete technische und organisatorische Maßnahmen gehören, existieren nützliche Referenzen wie etwa der BSI-Grundschutzkatalog oder das Österreichische Informationssicherheitshandbuch. Diese können dazu beitragen, sinnvolle Maßnahmen im Unternehmen umzusetzen.

6. WELCHE GOVERNANCE-VERPFLICHTUNGEN TREFFEN LEITUNGSORGANE ERFASSTER UNTERNEHMEN?

ALLGEMEINES

Unter den Governance-Verpflichtungen der NIS2-RL versteht man Verpflichtungen, welche die Leitungs- und Führungsebene (z.B. Vorstand*in einer AG, Geschäftsführer*in einer GmbH) des Unternehmens betreffen. Diese ist insbesondere für die Billigung und Überwachung der Umsetzung der Risikomanagement-Verpflichtungen verantwortlich und könnte bei Verstößen gegen dieselben auch persönlich (!) verantwortlich gemacht werden.

Um diesen Aufgaben auch entsprechend gerecht zu werden, werden Leitungsorgane zur Teilnahme an Schulungen verpflichtet. Diese haben sie auch ihren Mitarbeiter*innen anzubieten. Ziel dahinter ist es, dass ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen vermittelt werden und Gefahren so präventiv vorgebeugt wird.

BACKGROUND INFO

Die spezifischen Haftungsbestimmungen sind noch vom österreichischen Gesetzgeber bis zum 17. Oktober 2024 durch ein nationales Gesetz zu erlassen. Sofern diese speziellen Haftungsbestimmungen allerdings nicht anzuwenden sind, finden die allgemeinen Regelungen Anwendung.

PRAXISTIPP

Schulungen sollten regelmäßig und an aktuelle Gegebenheiten angepasst durchgeführt werden. Dies nicht nur, um Haftungen zu reduzieren, sondern bereits aus Eigeninteresse an einer höheren faktischen Sicherheit.

7. WELCHE MELDEVERPFLICHTUNGEN SIND EINZUHALTEN?

ALLGEMEINES

Eine Meldepflicht besteht vor allem bei erheblichen Sicherheitsvorfällen. In diesem Kontext spielen die Computer-Notfallteams (engl. „Computer Security Incident Response Teams“ oder auch „Computer Emergency Response Teams“ [kurz „CSIRT“]) eine wichtige Rolle. Sie sind für „die Prävention, Erkennung, Reaktion und Folgenminderung bei Risiken, Vorfällen und Sicherheitsvorfällen wichtig.[1]“

Wesentliche und wichtige Einrichtungen haben ihr CSIRT oder ggf. die Behörde unverzüglich über jeden Sicherheitsvorfall zu unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat. Wenn der Sicherheitsvorfall einen angebotenen Dienst beeinträchtigen könnte, hat die betreffenden Einrichtungen gegebenenfalls auch die Empfänger*innen ihrer Dienste unverzüglich über den Sicherheitsvorfall zu unterrichten. Die Meldepflicht umfasst dabei, unter anderem eine Frühwarnung, eine Folgemeldung sowie einen Zwischen- und Abschlussbericht.

Bei der Meldung sind unterschiedliche (Höchst-)Fristen zu beachten, die entweder 24 Stunden, 72 Stunden oder einen Monat betragen. Zu berücksichtigen ist hierbei, dass es sich bei diesen Fristen um Höchstfristen handelt und in den meisten Fällen eine unverzügliche Meldung gefordert wird.

Neben diesen Verpflichtungen zur Meldung besteht auch die Möglichkeit in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle, freiwillig Meldung an das CSIRT zu erstatten. Diese Option steht auch nicht wichtigen und nicht wesentlichen Einrichtungen zur Verfügung.

[1]Computer-Notfallteams (CSIRTs) im Sinne des NIS-Gesetzes; https://www.nis.gv.at/fragen-und-antworten/computer-notfallteams.html [zuletzt abgerufen am 21.02.2024].

BACKGROUND INFO

Das CSIRT wurde bereits durch die NIS-RL geschaffen und wird durch die NIS2-RL weiter ausgebaut. In Österreich sind aktuell für Private zwei CSIRT eingerichtet: das nationale CSIRT (Computer Emergency Response Team Austria, www.cert.at) sowie eines für den Energiesektor (AEC, www.energy-cert.at).

PRAXISTIPP

Neben den Meldeverpflichtungen der NIS2-RL können sich solche auch aus anderen Gesetzen ergeben.

Hier ist insbesondere auf die Meldeverpflichtungen der DSGVO zu verweisen. Insbesondere auf der Website von CERT.at finden sich zahlreiche cybersicherheitsrelevante, aktuelle (Prüf-)Berichte und Informationen.

Ebenfalls besteht die Möglichkeit zur Meldung an die „Watchlist Internet“, wodurch andere Unternehmen von der Bedrohung gewarnt werden können.

8. WAS DROHT BEI VERSTÖSSEN?

ALLGEMEINES

Bei einem Verstoß gegen Bestimmungen können bisweilen bedeutende Bußgelder verhängt werden. Für **wesentliche Einrichtungen** können Bußgelder mit einem Höchstbetrag von mindestens 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes verhängt werden. Für **wichtige Einrichtungen** (also alle anderen Einrichtungen die in den Anwendungsbereich der NIS2-RL fallen) beträgt das höchstmögliche Bußgeld mindestens 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes. Für beide gilt der jeweils höhere Betrag. Für die genauen Haftungsbestimmungen wird man allerdings auf die österreichische Umsetzung der Richtlinie warten müssen.

Neben allfälligen Bußgeldzahlungen kann die zuständige Behörde gem Art 32 Abs. 4 NIS2-RL noch weitere verbindliche Anweisungen und Anordnung setzen, um die Einhaltung der Richtlinie zu gewährleisten.

Sollte die betroffene Einrichtung diesen Anweisungen nicht Folge leisten, ist die Behörde dazu berechtigt, die Ausübung der einschlägigen Tätigkeit vorübergehend auszusetzen. Auch kann die Behörde Personen mit Geschäftsleitungsaufgaben (z. B.: Vorstand*in, Geschäftsführung) die Tätigkeit für die Einrichtung vorübergehend untersagen.

Darüber hinaus können Verstöße schadenersatzrechtliche Folgen nach sich ziehen.

Zu beachten ist weiters, dass Leitungsorgane (z. B.: Vorstand*in einer AG, Geschäftsführer*in einer GmbH) für die Einhaltung der Cybersicherheitsmaßnahmen persönlich haften können.

Ebenso ist zu bedenken, dass es zu einem Verlust des Versicherungsschutzes kommen kann, wenn die Verpflichtungen der NIS2-RL nicht eingehalten werden.

Neben all diesen rechtlichen Folgen bestehen auch weitere faktische Probleme, zu denen es bei einer Nicht-Umsetzung der Cybersicherheitsmaßnahmen kommen kann. Dazu zählen unter anderem ein Produktionsausfall, Explosionen und Brände, Erpressungen oder auch ein Datenverlust. Schadensbehebungskosten können ebenfalls substantielle Beträge erreichen.

BACKGROUND INFO

Der zuständigen Behörde stehen diverse Maßnahmen zur Verfügung um zu kontrollieren, ob es zu einem Verstoß gegen die Richtlinie gekommen ist. Zu diesen Maßnahmen zählen zum Beispiel: Vor-Ort-Kontrollen, regelmäßig durchgeführte als auch Ad-Hoc-Sicherheitsprüfungen, Sicherheitsscans, Anforderung von Informationen (Dokumente, etc.) sowie Anforderung von Compliance-Nachweisen.

PRAXISTIPP

Die Relevanz der persönlichen Haftung von Führungskräften ist in der Praxis besonders hoch. So sind sie nach einem Cyberangriff oft die einzigen Personen, die faktisch und wirtschaftlich zur Verantwortung gezogen werden können und daher für potentiell geschädigte besonders attraktive Haftungsziele.

PRAXISTIPP

Bis 15. April läuft noch die Ausschreibung der FFG (Forschungsförderungsgesellschaft) für Cyber Security Schecks. Diese Schecks unterstützen österreichische KMU, die zur Anwendung der Cybersicherheits-Richtlinie NIS2 verpflichtet sind, bei der Umsetzung von Cyber Security Maßnahmen zu NIS2 und sind eine Maßnahme des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT), das das BKA in Kooperation mit der FFG leitet. Die Förderung erfolgt in Form von nicht rückzahlbaren Zuschüssen und beträgt pro Cyber Security Scheck maximal 10.000 €. Die Förderquote beträgt maximal 40% der förderbaren Gesamtkosten des Projekts.

Mehr dazu auf
https://www.ffg.at/ausschreibung/CyberSecuritySchecks2023

Bei Rückfragen wenden Sie sich gerne an:
Dr. Arthur Stadler
Partner, Stadler Völkel Rechtsanwälte GmbH

Tel.: +43 1 997 10 25
arthur.stadler@sv.law

HAFTUNGSAUSSCHLUSS

IMPRESSUM

HANDELSVERBAND – Verband österreichischer Handelsunternehmen
Verein nach dem Vereinsgesetz 2002, zust. Vereinsbehörde. BPD Wien, ZVR: 688103413
Geschäftsführer: Ing. Mag. Rainer Will | **Präsident:** Dr. Stephan Mayer-Heinisch
Vizepräsidenten: Karin Saey, Mag. Harald Gutschi, Horst Leitner, Norbert W. Scheele, Andrea Heumann
Inhalt: Dr. Arthur Stadler, Mag. Nina Putz, Mag. Gerald Kühberger
Design: Gebrüder Pixel OG
+43 (1) 406 22 36 | office@handelsverband.at | www.handelsverband.at