4/2024
72 – 96

BVwG
Daten Fitness-App
Viktoria Haidinger/Michael Löffler

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Neue RL zur Cybersicherheit: NIS-2

NIS-2: ein Überblick
Michael Löffler

NIS-2: die Anwendung im Konzern
Rainer Knyrim und Stephanie Briegl

Checkliste NIS-2
Hans-Jürgen Pollirer

Effektiver Datenschutz erfordert Anstrengungen und Ressourcen
Interview mit Alma Zadić, Bundesministerin für Justiz

Das neue Medienprivileg (§ 9 DSG)
Rainer Knyrim

Recht auf Löschung eines Spielerfotos
Andreea Panazan

Recht auf Datenübertragbarkeit
Theresia Leitinger

ISSN 2313-5409

MANZ 175 Jahre

Michael Löffler
privacy awareness e.U.

NIS-2: ein Überblick

Netz- und Informationssysteme; Cybersicherheit. Der Beitrag verschafft einen raschen Überblick über den Anwendungsbereich der NIS-2-RL und Ausnahmen von diesem. Weiters werden zentrale Pflichten der Mitgliedstaaten bzw „wesentlicher" und „wichtiger" Einrichtungen dargestellt.

Anwendbarkeit

Im Unterschied zur NIS-RL bzw deren Umsetzung dem NISG, welches geprägt war von der bescheidmäßigen Zuschreibung der Eigenschaft „wesentlicher Dienst", an dem sich die Anwendbarkeit der Rechtsnormen knüpfte,[1] wählt die NIS-2-RL einen anderen Ansatz. Zukünftig werden Organisationen, die vorgegebenen Kriterien entsprechen (s sogleich), bereits **ex lege von NIS-2 erfasst**. Unterschieden wird zukünftig zwischen „wesentlichen" und „wichtigen" Einrichtungen (zu den Pflichten s unten).[2]

Organisationen, die den Kriterien entsprechen, werden ex lege von NIS-2 erfasst.

Zunächst erfasst werden Einrichtungen der in Anh I oder II genannten Art,[3] die ihre Dienste in der EU erbringen oder ihre Tätigkeit hier ausüben, ab einer bestimmten **Größe**. Auf diese Art erfasst werden Organisationen, die 50 Personen oder mehr beschäftigen und deren Jahresumsatz/Jahresbilanz 10 Mio Euro übersteigt. Anh I definiert Einrichtungen in Sektoren mit hoher Kritikalität und entspricht im Wesentlichen Anh II NIS-RL; er enthält aber einige neue Sektoren wie Abwasser, Verwaltung von IKT-Diensten (B2B) oder Weltraum. Anh II enthält sonstige kritische Sektoren wie Abfallbewirtschaftung, Produktion, Verarbeitung und Vertrieb von Lebensmitteln oder Forschung.

Weiters werden – **größenunabhängig** – näher **definierte Einrichtungen** der in Anh I oder II genannten Art erfasst.[4] Dies sind:

- Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten,
- Vertrauensdiensteanbieter,
- Namenregister der Domäne oberster Stufe und
- Domänennamensystem-Diensteanbieter.

Ebenso erfasst werden:

- Anbieter von Diensten, die für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich sind, sofern es sich um die einzigen Anbieter in einem MS handelt.
- Einrichtungen, bei denen sich eine Störung eines erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte.
- Einrichtungen, die aufgrund ihrer besonderen Bedeutung kritisch sind, die sie auf nationaler oder regionaler Ebene für einen betreffenden Sektor, die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in einem MS haben.

Im Bereich der **öffentlichen Verwaltung** werden in Österreich sämtliche Einrichtungen des Bundes erfasst.[5] Darüber hinaus zwingend aber auch Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.[6]

Der Anwendungsbereich der Cybersicherheitsvorschriften wurde im Vergleich zur Vorgängerregelung äußerst erweitert

Per Verweis auf die **RL** zum **Schutz kritischer Einrichtungen** (RL [EU] 2022/2557) werden sämtliche nach dieser Norm kritischen Einrichtungen auch von der NIS-2-RL erfasst.[7] Diese Regelung stellt sicher, dass sämtliche „kritische Einrichtungen" unabhängig von ihrer Größe erfasst werden. Größenunabhängig werden auch sämtliche Domänennamenregistrierungsdienste erfasst.[8]

MS können die Anwendung der NIS-2-RL schließlich ausdehnen auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen, insb wenn diese **kritische Forschungstätigkeiten** durchführen.[9]

Da zukünftig etwa auch Organisationen aus dem Bereich des Abwassers,[10] der Abfallbewirtschaftung,[11] Lebensmittelunternehmen[12] oder Forschungseinrichtungen[13] erfasst werden, wird sich die Zahl der betroffenen Organisationen wird sich deshalb von wenigen Hunderten auf einige Tausende erhöhen. Um Organisationen die Prüfung zu erleichtern, ob sie von NIS-2 betroffen sind, stellt die WKO einen **Online-Ratgeber** zur Verfügung.[14]

Ausnahmen vom Anwendungsbereich

Nicht von der NIS-2-RL erfasst werden Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche **Sicherheit**, **Verteidigung** oder **Strafverfolgung** ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten.[15] Einrichtungen, die in diesem Kontext tätig sind oder die Dienste in diesem Kontext für die öffentliche Verwaltung erbringen, können auf mitgliedstaatlicher Ebene von bestimmten Verpflichtungen der NIS-2-RL ausgenommen werden.[16] In diesem Fall gelten auch Aufsichts- und Durchsetzungsmaßnahmen (Kap VII NIS-2-RL) nicht.[17] Vertrauensdiensteanbieter können jedoch nicht unter Berufung auf diese Regelung von der NIS-2-RL ausgenommen werden.[18]

Ebenfalls nicht von der NIS-2-RL erfasst sind jene Einrichtungen, die von MS bereits vom Digital Operational Resilience Act (**DORA** – VO [EU] 2022/2554) erfasst wurden. Zur Verwirklichung des Ziels, ein gemeinsames hohes Niveau an digitaler operationaler

[1] Vgl § 16 NISG. [2] S Legaldefinition Art 3 NIS-2-L, vgl auch *Pollirer*, Checkliste NIS-2, Dako 2024/43 (in diesem Heft Seite 88). [3] Die Anh NIS-2-RL listen – tw uVa andere Rechtsakte – weitere Kriterien auf, die Einrichtungen erfüllen müssen, um erfasst zu werden (etwa das Erbringen bestimmter Dienste oder das Überschreiten von Schwellenwerten). [4] Vgl Art 2ff NIS-2-RL. [5] Vgl Art 2 Abs 2 lit f sublit i NIS-2-RL. [6] Vgl im Unterschied dazu die bisherige Regelung § 22 Abs 5 NISG, wonach Länder die Pflichten der § 22 Abs 1 und 2 NISG per Gesetz für anwendbar erklären konnten. [7] Art 3 Abs 2 NIS-2-RL. [8] Art 2 Abs 4 NIS-2-RL. [9] Art 5 NIS2-RL. [10] Vgl Anh I Z 7 NIS-2-RL. [11] Vgl Anh II Z 2 NIS-2-RL. [12] Vgl Anh II Z 4 NIS-2-RL. [13] Vgl Anh II Z 7 NIS-2-RL. [14] WKO, Online Ratgeber: Cybersicherheitsrichtlinie – NIS2; für Details zum Anwendungsbereich s *Knyrim/Briegl*, NIS-2: die Anwendung im Konzern, Dako 2024/39 (in diesem Heft Seite 78). [15] Art 2 Abs 7 NIS2-RL. [16] Derartige Einrichtungen können von den Verpflichtungen der Art 21 oder 23 NIS-2-RL ausgenommen werden. Sollten Einrichtungen ausschließlich Tätigkeiten im betreffenden Kontext ausüben oder entsprechende Dienste erbringen, können diese zusätzlich von den Verpflichtungen der Art 3 und 27 NIS-2-RL ausgenommen werden. [17] Art 2 Abs 8 NIS-2-RL. [18] Art 2 Abs 9 NIS-2-RL.

Resilienz zu erreichen, legt DORA Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen (iSd NIS-2-RL) fest. Die Regelungen von DORA und der NIS-2-RL sind in diesem Kontext vergleichbar; DORA gilt allerdings nur für den Finanzsektor.[19]

Pflichten von Mitgliedstaaten

Um die bereits durch die NIS-RL geschaffenen Rahmenbedingungen noch weiter zu verfeinern, enthält die NIS-2-RL eine Reihe von Pflichten für MS. Dadurch soll das Thema Cybersicherheit umfassend adressiert werden. Die ehemals in der NIS-RL vorgesehene Strategie für die Sicherheit von Netz- und Informationssystemen[20] hat zu einer **Cybersicherheitsstrategie** weiterentwickelt zu werden (Art 7 NIS-2-RL). Ein hervorzuhebender Punkt ist ein von MS zu erstellender Plan zur Steigerung der Sensibilisierung für Cybersicherheit bzw -hygiene bei Bürger:innen. Alle zwei Jahre hat die ENISA[21] in einem **Bericht** über den Stand der Cybersicherheit zu bewerten, wie es unionsweit um diese beiden Aspekte bei Bürger:innen steht.[22]

Ebenfalls neu ist, dass zusätzlich zu(r) für die Cybersicherheit zuständigen Behörde(n) eine oder mehrere für das Management von **Cybersicherheitsvorfällen großen Ausmaßes**[23] und Krisen zuständige Behörde(n) benannt bzw eingerichtet werden muss/müssen.[24] Um für die Bewältigung von Cybersicherheitsvorfällen großen Ausmaßes gewappnet zu sein, müssen MS auch einen entsprechenden Plan verabschieden.

Die Regelungen zu den bereits aus der NIS-RL bekannten **Computer-Notfallteams** (CSIRT)[25] wurden um solche zur gemeinsamen Zusammenarbeit ergänzt. Hervor sticht die Teilnahme von CSIRTs an freiwilligen, von Sachverständigen für Cybersicherheit durchgeführten **Peer Reviews.**[26] Ziel dieser Peer Reviews ist es, aus gemeinsamen Erfahrungen zu lernen und das gegenseitige Vertrauen zu stärken, um ein gemeinsames hohes Cybersicherheitsniveau zu erreichen. Hierzu werden ua der Stand der Umsetzung bestimmter NIS-2-Pflichten, die Kapazitäten von CSIRTs und spezifische Fragen mit grenz- oder sektorenübergreifendem Charakter von Sachverständigen geprüft.

Ein CSIRT hat in jedem MS als **Koordinator für Schwachstellen** benannt zu werden. Dieses fungiert als Drehscheibe zwischen Personen/Institutionen, die Schwachstellen (anonym) melden, und Herstellern/Anbietern der potenziell gefährdeten Produkte/Dienste.[27]

Auf europäischer Ebene wird ein aus Vertretern der Cybersicherheitsmanagementbehörden der MS und der EK bestehendes **Netzwerk der Verbindungsorganisationen für Cyberkrisen** (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) errichtet werden.[28] Ziel dieses Netzwerks ist es, Cybersicherheitsvorfälle großen Ausmaßes und Krisen koordiniert zu bewältigen und für einen regelmäßigen Austausch von Informationen zwischen den MS und Einrichtungen der EU zu sorgen.

Zur europaweiten Information hat die ENISA eine Schwachstellendatenbank zu führen.

Pflichten wesentlicher und wichtiger Einrichtungen

Sowohl für wesentliche als auch für wichtige Einrichtungen muss auf mitgliedstaatlicher Ebene eine Pflicht vorgesehen werden, Leitungsorgane und **Mitarbeitende** im Bereich der Cybersicherheit zu **schulen.**[29] Beide Einrichtungsarten werden auch dazu verpflichtet, unter Berücksichtigung des Stands der Technik, von Normen und Kosten, angemessene, geeignete technische, operative und organisatorische Maßnahmen zu ergreifen, um Cyberrisiken für ihre Dienste auszuschließen oder möglichst gering zu halten.[30] Dieser risikobasierte Ansatz ist Organisationen bereits aus der DSGVO (vgl Art 32) bekannt. Art 21 NIS-2-RL listet sodann Aspekte auf, die idZ jedenfalls berücksichtigt werden müssen, wie etwa Backup-Management, Kryptografiekonzepte, Multi-Faktor-Authentifizierung oder Personalsicherheit. Wesentliche und wichtige Einrichtungsarten treffen auch Berichtspflichten über erhebliche Sicherheitsvorfälle.[31]

Ebenfalls berücksichtigt werden müssen die **Sicherheit der Lieferkette** und Sicherheitsmaßnahmen beim Erwerb von Informationssystemen. Diese gesamthafte Betrachtung der Informationssicherheit ist mit dem Ansatz von Art 28 DSGVO vergleichbar, der datenschutzrechtlich Verantwortliche verpflichtet, nur mit Auftragsverarbeitern (Dienstleistern) zusammenzuarbeiten, die die Sicherheit personenbezogener Daten (ggf auch bei etwaigen von ihnen herangezogenen weiteren Auftragsverarbeitern) gewährleisten können.

Unterschiedliche Regelungen für wesentliche bzw wichtige Einrichtungen enthält die NIS-2-RL etwa im Bereich von **Aufsichts- und Durchsetzungsmaßnahmen.**[32] Einen weiteren Unterschied gibt es zB bei der Höhe von Geldbußen. Verstoßen wesentliche Einrichtungen gegen Art 21 oder 23 NIS-2-RL, kann eine **Geldbuße** von 10 Mio Euro oder 2% des weltweit erzielten Umsatzes des letzten Geschäftsjahrs verhängt werden – je nachdem, welcher Betrag höher ist. Bei wichtigen Einrichtungen reduzieren sich die Zahlen auf 7 Mio Euro bzw 1,4%.[33]

Sollte ein Verstoß gegen Art 21 und 23 NIS-2-RL zugleich auch eine Verletzung des Schutzes personenbezogener Daten darstellen (also einen „**Data Breach**" gem Art 4 Z 12 DSGVO), aufgrund welcher die datenschutzrechtlichen Aufsichtsbehörden (in Österreich die DSB) eine Strafe verhängen, darf aufgrund der NIS-2-RL keine weitere Strafe verhängt werden.[34]

Nationale Umsetzung

In Österreich ist die nationale Umsetzung der RL ausständig. Diese hat bis spätestens zum 17. 10. 2024 zu erfolgen.[35] Zuletzt konnte ein Mitte Juni eingebrachter Initiativantrag nicht die notwendige parlamentarische Mehrheit erzielen.[36] Die Opposition kritisierte an diesem insb die Konzentration von Kompetenzen im Innenministerium.[37] Angesichts des bevorstehenden Termins für die Wahl eines neuen Nationalrats Ende September 2024 scheint eine fristgerechte Umsetzung somit nicht mehr möglich.

Fazit

Die zunehmende Digitalisierung macht es notwendig, dem Thema Cybersicherheit mehr Aufmerksamkeit zu widmen. Bereits jetzt müssen alle Organisation, die personenbezogene Daten verarbeiten, gem Art 32 DSGVO geeignete Datensicherheitsmaßnahmen ergreifen, um eine angemessene Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der datenverarbeitenden Systeme sicherzustellen. Wegen des deutlich ausgeweiteten Anwendungsbereichs der NIS-2-RL müssen künftig tausende Or-

[19] Legaldefinition des Begriffs „Finanzunternehmen" s Art 2 Abs 1 DORA. [20] Vgl Art 7 NIS-RL. [21] Agentur der Europäischen Union für Cybersicherheit. [22] Vgl Art 18 NIS-2-RL. [23] Dies ist ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines MS übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei MS hat (Art 6 Z 7 NIS2-RL). [24] Art 9 NIS2-RL. [25] Die auch in der dt Sprachfassung verwendete Abkürzung ist auf die engl Bezeichnung „computer security incident response teams" zurückzuführen. [26] Vgl Art 19 NIS-2-RL. [27] Art 12 NIS-2-RL. [28] Art 16 NIS-2-RL. [29] Art 20 NIS-2-RL. [30] Art 21 NIS-2-RL. [31] S Art 23 NIS-2-RL. [32] Vgl Art 32, Art 33 NIS-2-RL. [33] Art 34 NIS-2-RL. [34] Art 35 Abs 2 NIS-2-RL. [35] Art 41 NIS-2-RL. [36] 4129/A 27. GP. [37] *Parlamentskorrespondenz,* Nationalrat: Absage für Informationssystemsicherheitsgesetz.

ganisationen hohe Sicherheitsanforderungen auch iZm mit sonstigen Daten erfüllen.

Praxistipp

Datenschutz und Informationssicherheit sollten organisationsintern gemeinsam behandelt werden. Denn Maßnahmen zur Steigerung der Informationssicherheit erhöhen das Datenschutzniveau und umgekehrt.

Dako 2024/38

Zum Thema

Über den Autor

DI Michael Löffler ist Datenschutzexperte bei privacy awareness e.U.
E-Mail: michael.loeffler@privacyawareness.at

Links (Stand aller Links 5. 8. 2024)

- EUR-Lex: NIS-2-RL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32022L2555
- WKO Online Ratgeber NIS-2: https://ratgeber.wko.at/nis2/
- Parlamentskorrespondenz, Nationalrat: Absage für Informationssystemsicherheitsgesetz; www.parlament.gv.at/aktuelles/pk/jahr_2024/pk0785

Rainer Knyrim/Stephanie Briegl
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte

NIS-2: die Anwendung im Konzern

Netz- und Informationssysteme; Cybersicherheit; Konzernbetroffenheit. Der Beitrag analysiert Unklarheiten, die sich bei der Anwendung der NIS-2-RL (und dem österr Gesetzesentwurf) auf Konzerne ergeben.

Einleitung

Dieser Beitrag behandelt die **Einstufung von Konzerngesellschaften** in der NIS-2-RL. Der Anwendungsbereich der NIS-2-RL scheint auf den ersten Blick klar definiert zu sein, allerdings ergeben sich bei genauerer Beschäftigung einige Fragen für die Einstufung von einzelnen Konzerngesellschaften und der **Anwendbarkeit im Konzern** im Allgemeinen. Allen voran geht es um Fragen zur Einstufung von Erbringern von Dienstleistungen für Konzerngesellschaften (va Konzern-Rechenzentrumsdiensten) und die Anwendbarkeit von Ausnahmen, die für verbundene Unternehmen unter Berechnung der Schwellenwerte herangezogen werden. Aber auch die Einstufung von Gesellschaften, die einen nur untergeordneten Teil ihrer Geschäftstätigkeit in einem NIS-2-relevanten Sektor erbringen oder von ausländischen Gesellschaften, die in Europa tätig sind, bereitet Schwierigkeiten. Diese Unklarheiten werden im Folgenden adressiert.

Fehlende Konzernregelung

Bei Unternehmen mit einer komplexeren Struktur (Konzern, zB Mutter- und Tochtergesellschaft) ist die Frage einer konzernweiten Betroffenheit schwierig zu beantworten, weil viele Bestimmungen der bisher bestehenden rechtlichen Regelungen (NIS-2-RL, österr Gesetzesentwurf) bei näherer Betrachtung Unklarheiten aufweisen. Der Anwendungsbereich der NIS-2-RL für die Einstufung von Konzernen ist nicht abschließend geregelt. Die NIS-2-RL enthält grundsätzlich keine Konzernregelung, sondern spricht lediglich vom **Begriff der „Einrichtung"** in Art 6 Z 38 NIS-2-RL.

Bei Konzernen ist einer „Einrichtung" nicht immer nur eine juristische Person zugeordnet.

Der NIS-2-RL zufolge sollen primär nur jene Einrichtungen unter den Anwendungsbereich fallen, die auch tatsächlich die Tätigkeiten ausüben oder die Dienste erbringen, die den sachlichen Anwendungsbereich der RL eröffnen.[1] Vereinfacht gesagt bedeutet dies: Wenn ein Unternehmen in den relevanten Sektoren tätig ist und die erforderliche Größe aufweist, fällt es unter die NIS-2-RL. Wie bisher in der Lit bereits kritisch angemerkt wurde, entsteht durch die NIS-2-RL aber der Eindruck, dass einer „Einrichtung" immer nur eine dahinterstehende juristische Person zugeordnet ist. Bei Blick auf Konzernstrukturen wird jedoch schnell deutlich, dass dies jedenfalls nicht der Realität entspricht.[2]

Erbringung konzerninterner Dienstleistungen

So bestehen etwa für IT-Konzerngesellschaften und deren Einstufung als Anbieter von **Rechenzentrumsdiensten** im Konzern einige **Abgrenzungsprobleme**. Nach der in der NIS-2-RL in Art 6 Z 31 enthaltenen Definition ist ein Rechenzentrumsdienst jeder *„Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die Zentrale und Erbringung, die Verbindung und den Betrieb von IT und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen, Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden"*. ErwGr 35 NIS-2-RL soll diese weite Definition offenbar etwas einschränken und sieht vor, dass von dem Begriff des Rechenzentrumsdiensts interne Rechenzentren nicht umfasst sein sollen, die sich im Besitz der betreffenden Einrichtung befinden und von dieser für eigene Zwecke betrieben werden.

Im Zuge einer strengen **Wortlautinterpretation** ergibt sich jedoch, dass bei der Erbringung von Dienstleistungen iSe Rechenzentrums, das von einer GmbH intern betrieben wird, der Anwendungsbereich der NIS-2-RL bei Fehlen der weiteren Voraussetzungen nicht eröffnet,[3] bei der Erbringung von Rechenzentrumsdiensten durch eine GmbH für eine andere Konzern-GmbH bei Erfüllung der weiteren Voraussetzungen durch diese GmbH aber schon eröffnet ist.[4] Da die Auslagerung der Er-

[1] *Hessel/Callewaert/Schneider,* Die NIS-2-RL aus Unternehmensperspektive, RDi 2024, 208. [2] *Leßner/Mayr,* Besonderheiten für Konzerne in den NIS-Richtlinien und dem BSIG, MMR 2024, 148; *Hessel/Callewaert/Schneider,* RDi 2024, 208. [3] *Hessel/Callewaert/Schneider,* RDi 2024, 208.