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

verarbeitete Daten einschlägig, die auf Rechtsgrundlage einer **Einwilligung** oder eines **Vertrags** beruhen. Eine Ausdehnung der Rechtsgrundlage in Form einer Analogie ist ausgeschlossen. Der Anspruch richtet sich ausschließlich gegen **Verantwortliche**. In der Praxis spielt das Recht auf Datenübertragbarkeit (noch) keine große Rolle, was wohl dem **engen Anwendungsbereich** geschuldet ist. Mit Spannung abzuwarten bleiben **zukünftige technische Entwicklungen** und wie Gerichte und Behörden auf diese reagieren, da mit voranschreitender Digitalisierung eine Zunahme der Geltendmachung dieses Rechts erwartbar ist.

Dako 2024/42

Zum Thema

Über die Autorin

MMag.[a] Dr.[in] Theresia Leitinger, M.A.I.S., ist Rechtsanwältin und Partnerin der Dr. Leitinger & Dr. Leitinger Rechtsanwälte GmbH in Graz, sie ist spezialisiert im Datenschutzrecht.
E-Mail: tl@ra-leitinger.at

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste NIS-2

Anwendungsbereich; risikobasierter Ansatz; Dokumentation; Qualitätsmanagementsystem; Transparenzpflichten. Die Checkliste soll Unternehmen bei der Umsetzung der NIS-2-RL und des nationalen Umsetzungsgesetzes NISG unterstützen. Von der NIS-2-RL sind schätzungsweise mehr als 5.000 Organisationen/Unternehmen sowie 50.000 Unternehmen, die diese Gruppe als Lieferanten versorgen, betroffen.

NIS-2-RL

Die NIS-2-RL (RL[EU] 2022/2555 des EP und des Rates vom 14. 12. 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)[1] ist die Nachfolgerin der ursprünglichen RL für die Netz- und Informationssicherheit aus dem Jahr 2016,[2] die am 28. 12. 2018 mit dem NISG[3] umgesetzt wurde. Die aufgrund der Bestimmungen des § 4 Abs 2 NISG erforderliche Netz- und Informationssystemsicherheitsverordnung (NISV)[4] wurde am 17. 7. 2019 verlautbart.

Die Definition der neuen NIS-2-RL wurde deshalb notwendig, weil die ursprüngliche NIS-RL nicht einheitlich in den MS umgesetzt wurde und dadurch ein fragmentiertes Regelwerk entstand. Mit der NIS-2-RL sollen nun diese **Unzulänglichkeiten** durch folgende wesentliche Ziele **beseitigt** werden:

- Harmonisierung und Verbesserung des Sicherheitsniveaus in den MS;
- Definition und Umsetzung von Cybersicherheitsstrategien sowie von Risikomanagement-Abläufen;
- verschärfte Sanktionen bei Verstößen;
- zuverlässige Meldung von Sicherheitsvorfällen bei den zuständigen Stellen;
- Gewährleistung der durchgängigen Bereitstellung kritischer Dienste;
- Definition und Umsetzung von Sicherheitsmaßnahmen für die Lieferkette, um die Sicherheit externer Anbieter zu überprüfen und zu gewährleisten;
- Implementierung eines Asset-Managements, um kritische Informationssysteme zu identifizieren und zu schützen.

Anwendungsbereich

Darüber hinaus wurde der Anwendungsbereich, wie die Abb 1 (Seite 89) zeigt, wesentlich erweitert. Im Unterschied zur ursprünglichen NIS-RL wurden die von der NIS-2-RL betroffenen Einrichtungen in **„wesentliche Einrichtungen"**, die einer strengen ex-ante- und ex-post-Aufsicht (Art 32 NIS-2-RL) sowie in **„wichtige Einrichtungen"**, die nur einer ex-post-Aufsicht (Art 33 NIS-2-RL) unterliegen, unterteilt. Des Weiteren wächst auch die Forderung nach mehr Cybersicherheit stetig und erfordert neue Maßnahmen, um die **Entwicklung der Bedrohungslandschaft** und der **steigenden Cyberkriminalität** entgegenzuwirken. Waren von der NIS-RL noch rund 100 Organisationen und Unternehmen in Österreich betroffen,[5] so gilt NIS-2 für mehr als 5.000 Organisationen und Unternehmen sowie für schätzungsweise 50.000 Unternehmen, die diese Gruppe als Lieferanten versorgen.[6]

Als Betroffene gelten mittlere und große Unternehmen bestimmter Sektoren sowie die digitale Infrastruktur. Die Klassifizierung der Unternehmensgröße basiert auf Empfehlungen und Definitionen der EK für KMU.

[1] https://kurzlinks.de/75c5. [2] RL (EU) 2016/1148, https://kurzlinks.de/2hur. [3] www.ris.bka.gv.at/dokumente/bgblauth/bgbla_2018_i_111/bgbla_2018_i_111.pdfsig. [4] www.ris.bka.gv.at/dokumente/bgblauth/bgbla_2019_ii_215/bgbla_2019_ii_215.pdfsig. [5] www.wko.at/it-sichherheit/nis2. [6] www.cxber-trust.at/nis/.

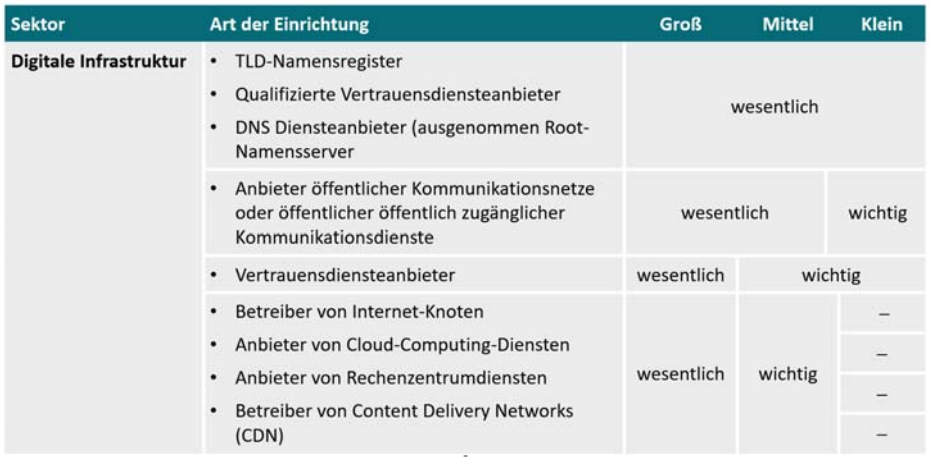
Betroffene Sektoren

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, **Fernwärme/Kälte,** Öl, Gas und **Wasserstoff**)	**Post- und Kurierdienste**
Verkehr (Luft, Schiene, Schifffahrt, Straße)	**Abfallbewirtschaftung**
Bankwesen	**Chemie (Herstellung und Handel)**
Finanzmarktinfrastrukturen	**Lebensmittel (Produktion, Verarbeitung, Vertrieb)**
Gesundheitswesen (Gesundheitsdienstleister, **EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte**)	**Verarbeitendes/herstellendes Gewerbe (Medizinprodukte; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)**
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und **soziale Netzwerke**)
Abwasser	**Forschung**
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, **Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze und dienste**)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Tab 1: Unterteilung der betroffenen Sektoren. **Fett hervorgehoben** = Neuerungen gegenüber NIS1. Quelle: bundeskanzleramt.gv.at

Größenklasse	Mitarbeiter (VZÄ)	Jahresumsatz	Jahresbilanzsumme
Klein (KU)	< 50 und	≤ 10 Mio EUR oder	≤ 10 Mio EUR
Mittel (MU)	< 250 und	≤ 50 Mio EUR oder	≤ 43 Mio EUR
Groß (GU)	≥ 250 oder	> 50 Mio EUR und	> 43 Mio EUR

Tabelle 2: Klassifizierung der Unternehmensgröße



Sektor	Art der Einrichtung	Groß	Mittel	Klein
Digitale Infrastruktur	• TLD-Namensregister • Qualifizierte Vertrauensdiensteanbieter • DNS Diensteanbieter (ausgenommen Root-Namensserver	wesentlich		
	• Anbieter öffentlicher Kommunikationsnetze oder öffentlicher öffentlich zugänglicher Kommunikationsdienste	wesentlich		wichtig
	• Vertrauensdiensteanbieter	wesentlich	wichtig	
	• Betreiber von Internet-Knoten • Anbieter von Cloud-Computing-Diensten • Anbieter von Rechenzentrumdiensten • Betreiber von Content Delivery Networks (CDN)	wesentlich	wichtig	– – – –

Abb: Anwendungsbereich

KU fallen nicht unter die NIS-2-RL, außer es handelt sich um:

- Vertrauensdiensteanbieter;
- Anbieter öffentlicher Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste;
- TLD-Namensregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namensservern;
- Unternehmen, die alleiniger Anbieter eines Service in einem MS sind, das essentiell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.

Darüber hinaus sind auch **Zulieferer** und **Dienstleister** von NIS-2-RL-Unternehmen durch die Verpflichtung zur Gewährleistung der Sicherheit der Lieferkette ihrer Kunden verpflichtet, Cybersecurity-Maßnahmen umzusetzen (Art 22 NIS-2-RL).

Art 21 Abs 5 NIS-2-RL sieht vor, dass die EK bis zum 17. 10. 2024 Durchführungsrechtsakte zu den in Art 21 Abs 2 NIS-2-RL angeführten zehn Maßnahmen zum Schutz der Netz- und Informationssysteme vor Sicherheitsvorfällen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter erlässt.

Gem Art 21 NIS-2-RL haben die MS sicherzustellen, dass die wesentlichen und wichtigen Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, und zwar unter Berücksichtigung des

- Stands der Technik,
- europäischer internationaler Normen und
- des bestehenden Risikos.

Diese Maßnahmen müssen gem Art 21 Abs 2 NIS-2-RL zumindest Folgendes umfassen:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Strafen

Verstöße gegen die Bestimmungen der NIS-2-RL können für wesentliche Einrichtungen mit einer maximalen Geldbuße in Höhe von 10 Mio Euro oder 2% des weltweiten Umsatzes sanktioniert werden, je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen beträgt die maximale Höhe der Geldbuße 7 Mio Euro oder 1,4% des weltweiten Umsatzes, je nachdem, welcher Betrag höher ist.

Umsetzung

Die NIS-2-RL ist am 16. 1. 2023 in Kraft getreten und von den EU-MS bis 17. 10. 2024 in nationales Recht umzusetzen. Der österr Gesetzgeber legte am 3. 4. 2024 den Entwurf des Netz- und Informationssystemsicherheitsgesetzes 2024 (NISG 2024) vor, der am 19. 6. 2024 mit den Stimmen der ÖVP und der Grünen mehrheitlich den Innenausschuss passierte. Bei der am 3. 7. 2024 stattgefundenen Abstimmung im Parlament fand sich allerdings keine Zweidrittelmehrheit für das NISG 2024. Das NISG 2024 wurde daher vorerst nicht beschlossen. Bedingt durch die am 29. 9. 2024 stattfindenden Wahlen zum NR, wird es daher zu einer entsprechenden **Verzögerung** bei der Umsetzung der NIS-2-RL in nationales Recht kommen.

Die nachfolgende Checkliste soll Unternehmen bei der Umsetzung der NIS-2-RL und des nationalen Umsetzungsgesetzes NISG unterstützen. Grundsätzlich empfiehlt sich bei der Umsetzung der im NISG Anl III „Risikomanagementmaßnahmen" angeführten Bereiche eine Orientierung an den internationalen Vorgaben der ISO/IEC-27000-Normenreihe, im Besonderen der ISO/IEC 27001 und ISO/IEC 27002. Die NIS-Behörde, das ist die Abteilung IV/10 Netz- und Informationssystemsicherheit im BMI, die neben der strategischen NIS-Behörde im BKA als operative NIS-Behörde agiert, empfiehlt Betrieben **wesentlicher** Dienste neben der ISO/IEC 27001 und dem österreichischen Informationssicherheitshandbuch[7] noch folgende Informationssicherheitsstandards sowie **Best Practices**:

- IEC 62443 2–1: Supply Chain Security,
- CIS CSC v8.0,
- KSÖ Cyber Risk Rating: Anforderungen für A- bzw B-Rating.

[7] www.sicherheitshandbuch.gv.at/.

Prüffragen

Prüffrage	ja	nein
Frage 1: Ist Ihre Organisation bzw Ihr Unternehmen von den Bestimmungen des NISG überhaupt betroffen? ***Anmerkung:*** *Wie die NIS-2-RL sieht das NISG grundsätzlich eine „Size-Cap-Rule" vor. Mit den §§ 24, 25 und 26 NISG werden die Bestimmungen des Art 3 NIS-2-RL in nationales Recht umgesetzt und jene Einrichtungen genannt, die in den Anwendungsbereich des NISG fallen. Wurden die betroffenen Organisationen und Unternehmen bei der NIS-RL noch vom BMI mittels Bescheid informiert, dass sie dieser RL unterliegen, müssen sie sich bei der NIS-2-RL selbst darum kümmern. § 24 Abs 1 Z 1 NISG führt jene Anbieter und Einrichtungen an, die als wesentliche Einrichtungen unabhängig von ihrer Unternehmensgröße gelten. Gem § 24 Abs 1 Z 2 NISG gelten auch Einrichtungen, die ein mittleres Unternehmen gem § 25 Abs 3 betreiben und Anbieter öffentlicher Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Telekommunikationsdienste als wesentliche Einrichtungen sowie auch Einrichtungen, der in Anlage 1 (Sektoren mit hoher Kritikalität) genannten Art, die ein großes (§ 25 Abs 2 NISG) oder mittleres (§ 25 Abs 3 NISG) Unternehmen betreiben. In § 24 Abs 2 NISG werden jene Einrichtungen, die in Anlage 1 und Anlage 2 (sonstige kritische Sektoren) angeführt sind, die ein großes oder mittleres Unternehmen betreiben, sowie Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen Kommunikationsdiensten, Vertrauensdiensteanbieter sowie Einrichtungen, die von der Cybersicherheitsbehörde (gem § 4 NISG nimmt diese Rolle das BMI wahr) als wichtige Einrichtungen eingestuft wurden. Der § 24 Abs 3, 4, 5 und 6 enthält die vom NISG betroffenen Einrichtungen im Sektor öffentliche Verwaltung.* *Die WKO hat einen Online-Ratgeber veröffentlicht, mit dem österr Unternehmen prüfen können, ob sie von der NIS-2-RL betroffen und daher zur Umsetzung der Maßnahmen verpflichtet sind.*[8]		
Frage 2: Sind sich die Leitungsorgane ihrer Rolle und ihrer Verantwortlichkeit bewusst? ***Anmerkung****: Verantwortlich für die Einhaltung der im NISG normierten Pflichten sind grundsätzlich gem § 31 Abs 1 NISG die Leitungsorgane (Vorstände und Aufsichtsrat bei einer AG, Geschäftsführer bei einer GmbH). Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen gem § 31 Abs 2 NISG an für sie spezifisch gestalteten Cybersicherheitsschulungen teilnehmen. Die Einrichtungen haben auch den Mitarbeitern gem § 31 Abs 2 NISG regelmäßig entsprechende Schulungen im Bereich Cybersicherheit anzubieten. Ein Verstoß gegen diese Bestimmungen wird gem § 45 Abs 2 NISG bei wesentlichen Einrichtungen mit einer Geldbuße bis 10 Mio Euro oder 2% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, je nachdem, welcher Betrag höher ist, sanktioniert. Bei wichtigen Einrichtungen beträgt die Geldbuße bis zu 7 Mio Euro oder 1,4%. Das österreichische Informationssicherheitshandbuch setzt sich unter Pkt 6.1.1 mit dem Thema „Managementverantwortung" auseinander. Die ISO/IEC 27002 führt hierzu die Maßnahme 5.4 an.*		
Frage 3: Wurde in Ihrer Organisation bzw Ihrem Unternehmen eine verantwortliche Person für die Informationssicherheit ernannt? ***Anmerkung:*** *In der Organisation bzw im Unternehmen sollte ein gesamtverantwortlicher Manager für die Informationssicherheit ernannt werden, der die gesamte Verantwortung für die Entwicklung und Umsetzung der Informationssicherheit übernimmt (Chief Information Security Officer, CISO). Er ist für das Risikomanagement sowie die sichere Entwicklung und Architektur der eingesetzten Sicherheitslösungen verantwortlich. Abhängig von der Größe und den Ressourcen der Organisation bzw des Unternehmens kann unter dem CISO die Informationssicherheit durch spezifische Funktionen oder Aufgaben abgedeckt werden.* *Das österreichische Informationssicherheitshandbuch setzt sich unter Pkt 3.1 „Verantwortung der Managementebene" mit diesem Thema ausführlich auseinander. Die ISO/IEC 27002 enthält hierzu die Maßnahmen 5.2 und 5.3.*		
Frage 4: Verfügt Ihre Organisation bzw Ihr Unternehmen über eine Sicherheitsrichtlinie? ***Anmerkung:*** *Die Sicherheitsrichtlinie ist ein wichtiges Grundsatz-Dokument, das die für die Organisation bzw das Unternehmen relevanten Sicherheitsziele und die Strategien in Form einer für alle verbindlichen Informationssicherheitspolitik (Information Security Policy) festlegt.*[9] *Sie ist von der Geschäftsleitung zu genehmigen, zu veröffentlichen und dem zuständigen Personal mitzu-*		

[8] https://ratgeber.wko.at/nis2/. [9] Details s Pollirer in Knyrim, DatKomm Art 32 Rz 32, 33 (Stand Mai 2022).

Prüffrage	ja	nein
teilen. Bei Bedarf ist die Informationssicherheitspolitik durch themenspezifische Richtlinien, die bestimmte Sicherheitsbereiche abdecken, zu unterstützen. Die ISO/IEC 27002 enthält umfangreiche Anforderungen im Bereich der Informationssicherheitspolitik und der Richtlinien mit den Maßnahmen 5.1 bis 5.3.		
Frage 5: Verfügt Ihre Organisation bzw Ihr Unternehmen über ein Risikomanagement-System? ***Anmerkung:*** *Unter einem Risikomanagement-System wird die Gesamtheit der Grundsätze, Verfahren und Maßnahmen verstanden, die einen strukturierten Umgang mit Risiken aller Art bewältigen. Im Wesentlichen umfasst das Risikomanagement-System die Risikoanalyse und die Risikobehandlung. Mit der Risikoanalyse wird versucht, die Sicherheitsrisiken zu erkennen und zu bewerten, während die Risikobehandlung den Prozess bezeichnet, bei dem Maßnahmen ausgewählt und geeignete organisatorische und technische Sicherheitsmaßnahmen (TOM) festgelegt und umgesetzt werden. Bevor eine Risikoanalyse durchgeführt wird, sind Risikoanalyse-Strategien in der Risikomanagement-Richtlinie festzulegen, wobei als mögliche Strategien die detaillierte Risikoanalyse, der Grundschutzansatz und der kombinierte Ansatz zu nennen sind.*[10] *Die Wirksamkeit der gewählten Strategie sollte laufend überprüft werden sowie auch die Einhaltung der in der Risikomanagement-Richtlinie festgelegten Vorgaben.* *Das österreichische Informationssicherheitshandbuch enthält in Punkt 5 „Risikomanagement" detaillierte Informationen zu diesem Thema. Va die ISO-Normen 31000 und 27005 setzen sich mit dem Thema Risikomanagement auseinander.*		
Frage 6: Gibt es in Ihrer Organisation bzw in Ihrem Unternehmen ein Inventar der Vermögenswerte (Assets) und wurden diese klassifiziert? ***Anmerkung:*** *Die ISO/IEC 27002 unterteilt die Assets in Primärwerte, das sind Informationen, Geschäftsprozesse und -aktivitäten, sowie die unterstützenden Werte (von denen die Primärwerte abhängen) wie Hardware, Software, Netzwerke, Personal, Standort und Struktur der Organisation. Die Informationen und Geschäftsprozesse sind entsprechend den Informationssicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit zu strukturieren (klassifizieren). Zu jedem Vermögenswert muss eine Verantwortlichkeit festgelegt werden, die die Verantwortung für die Verwaltung und die Sicherheit des Vermögenswerts trägt. Für den Umgang mit Wechseldatenträgern (USB-Sticks, USB-Festplatten oder DVD-ROM) sind besondere Sicherheitsmaßnahmen zu treffen. Weiters sind für das Löschen von Informationen entsprechende Verfahren festzulegen.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 8 ausführliche Informationen zum Thema „Vermögenswerte und Klassifizierung von Informationen". Die ISO/IEC 27002 führt hierzu die Maßnahmen 5.9 bis 5.13 an.*		
Frage 7: Werden von Ihrer Organisation bzw von Ihrem Unternehmen im Bereich der „Personellen Sicherheit" entsprechende Maßnahmen getroffen? ***Anmerkung:*** *Bewerber sollten grundsätzlich vor Aufnahme des Beschäftigungsverhältnisses – unter Einhaltung der entsprechenden gesetzlichen Bestimmungen und der ethischen Grundsätze – einer Sicherheitsprüfung unterzogen werden. Durch Verpflichtung aller Mitarbeiter auf die Einhaltung der einschlägigen Gesetze (wie zB § 6 DSG) und Richtlinien (wie zB Clear-Desk-Policy, Internetnutzung) sowie ausreichende Schulungsmaßnahmen im Bereich der Informationssicherheit soll sichergestellt werden, dass alle Mitarbeiter für die Aufgaben, für die sie vorgesehen sind oder die sie bereits wahrnehmen, geeignet sind und über das für ihre Aufgaben notwendige Sicherheitsbewusstsein verfügen. Für die Beendigung eines Beschäftigungsverhältnisses ist ein entsprechender Prozess zum Schutz der Organisation bzw des Unternehmens einzurichten. Für Verstöße gegen die Bestimmungen der Informationssicherheitspolitik oder der spezifischen Richtlinien ist eine Vorgehensweise zu definieren, die eine abschreckende Wirkung zur Prävention von Sicherheitsverletzungen vorsieht.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 7 „Personelle Sicherheit" detaillierte Ausführungen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahme 6 an.*		
Frage 8: Verfügt Ihre Organisation bzw Ihr Unternehmen über ausreichende Cybersicherheitskompetenzen? ***Anmerkung****: Die Sensibilisierung und Schulung der Mitarbeiter in Bezug auf das Thema „Cybersecurity" ist ein kritischer Faktor, um NIS-2-Compliance zu erreichen. Durch wirksame Schulungen, im Rahmen derer die Mitarbeiter über die neuesten Cyberbedrohungen informiert und in sicheren Verhaltensweisen geschult werden, ist entsprechende Cybersecuritykompetenz aufzubauen. Dabei ist es wichtig, dass alle Mitarbeiter regelmäßig geschult werden und auf den aktuellen Stand der Cybersicherheitspraktiken durch Aufnahme von Best-Practice-Beispielen in die Schulung gebracht werden.* *Als Ergänzung empfiehlt sich die Durchführung von Phishing-Tests bei den Mitarbeitern.* *Das österreichische Informationssicherheitshandbuch setzt sich mit diesem Thema unter Pkt 7.3. „Sicherheitssensibilisierung und -schulung" auseinander. Die ISO/IEC 27002 führt hierzu die Maßnahme 6.3 an.*		
Frage 9: Verfügt Ihre Organisation bzw Ihr Unternehmen über eine Richtlinie zur Sicherheit in der Lieferkette? ***Anmerkung:*** *Organisationen bzw Unternehmen sind zunehmend von der Informationssicherheit in der IKT-Lieferkette abhängig. Ein Sicherheitsvorfall bei einem Lieferanten von IKT-Dienstleistungen kann daher erhebliche Auswirkungen auf die betroffene Organisation bzw das betroffene Unternehmen haben. Um diese Risiken zu minimieren, sind zur Aufrechterhaltung eines erforderlichen Niveaus der Informationssicherheit in Lieferantenbeziehungen entsprechende Prozesse und Verfahren festzulegen und umzusetzen. So sind die Sicherheitsanforderungen va in der Vertragsgestaltung mit den IKT-Lieferanten zu berücksichtigen und Überwachungsprozesse einzurichten.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 15 „Lieferantenbeziehungen" detaillierte Ausführungen zu diesem Thema, wie auch die ISO/IEC 27002 mit den Maßnahmen 5.19 bis 5.23.*		
Frage 10: Verfügt Ihre Organisation bzw Ihr Unternehmen über eine Zugriffskontrollpolitik (Zugangssteuerung)? ***Anmerkung:*** *Durch eine Zugriffskontrollpolitik soll sichergestellt werden, dass der Zugang zu Informationen und anderen Vermögenswerten wie IT-Systemen, Netzwerken und Programmen entsprechend den Anforderungen der Organisation bzw des Unternehmens – unter Beachtung des „Need-to-Know"-Prinzips – definiert und autorisiert werden. Die Verfahren zur Vergabe und zum Entzug von Zugriffsrechten, die Verwaltung der Zugriffsrechte, das Identifikations-Management sowie die verwendeten Authentisierungsmethoden sind zu dokumentieren.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 9 „Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung" detaillierte Informationen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahme 5.15 an.*		
Frage 11: Verfügt Ihre Organisation bzw Ihr Unternehmen über ein Konfigurations- und -änderungsmanagement? ***Anmerkung:*** *Durch das Konfigurationsmanagement soll sichergestellt werden, dass die Konfiguration aller Systemkomponenten (Hardware, Software, Dienste und Netzwerke) festgelegt, dokumentiert, umgesetzt, überwacht und überprüft wird. Durch das Konfigurationsmanagement können Änderungen nachvollzogen und somit die Integrität und Leistungsfähigkeit des Systems über dessen gesamten Lebenszyklus sichergestellt werden.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 12 „Sicherheitsmanagement im Betrieb" ausführliche Informationen zu diesem Thema. Die ISO/IEC 27002 setzt sich mit der Maßnahme 8.9 mit dem Konfigurationsmanagement auseinander.*		
Frage 12: Verfügt Ihre Organisation bzw Ihr Unternehmen über Prozesse zur Verwaltung von identifizierten Schwachstellen und zur Reaktion auf Sicherheitsvorfälle (Incident Handling)? ***Anmerkung:*** *Grundsätzlich sollte die Organisation bzw das Unternehmen den Umgang mit Sicherheitsvorfällen planen und vorbereiten. Das bedingt die Einrichtung von Prozessen, die Festlegung von Verantwortlichkeiten sowie die Definition der notwendigen Maßnahmen. Detaillierte Vorgaben sollten in einem Incident-Handling-Plan dokumentiert werden.*		

[10] Details s *Pollirer* in *Knyrim*, DatKomm Art 32 Rz 35, 36 (Stand Mai 2022).

Prüffrage	ja	nein
Das österreichische Sicherheitshandbuch enthält unter Pkt 16 „Sicherheitsvorfälle bzw Informationssicherheitsereignisse (Incident Handling)“ detaillierte Informationen zu diesem Thema. Die ISO/IEC 27002 enthält hierzu die Maßnahmen 5.24 bis 5.30.		
Frage 13: Wurden in Ihrer Organisation bzw Ihrem Unternehmen bereits Prozesse implementiert, die eine rechtzeitige Meldung von Cyberangriffen gewährleisten? ***Anmerkung:*** *Wesentliche und wichtige Einrichtungen haben nach den Bestimmungen des § 34 NISG dem für sie zuständigen CSIRT oder den für sie zuständigen CSIRTs unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, nach Kenntnisnahme eines erheblichen Cybersicherheitsvorfalls eine Frühwarnung zu übermitteln und innerhalb von 72 Stunden eine aktualisierte Meldung, die bereits wesentliche Informationen über die Auswirkungen des Sicherheitsvorfalls enthält, abzugeben und schlussendlich einen Monat nach Abgabe der Meldung einen endgültigen Endbericht vorzulegen.*		
Frage 14: Führt Ihre Organisation bzw Ihr Unternehmen regelmäßige Sicherheitstests durch? ***Anmerkung:*** *Zur Gewährleistung der Sicherheit sollten Sicherheitstests – va bei neu angeschaffter Software oder bei Änderungen an der implementierten Software – durchgeführt werden. Sicherheitstests gewährleisten, dass die Anwendung, das Netzwerk und die Server frei von Sicherheitsmängeln sind und nicht zu einem Totalverlust der Informationen führen.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 14.1 „Sicherheit im gesamten Lebenszyklus eines IT-Systems“ detaillierte Informationen zu diesem Thema. Die ISO/IEC 27002 enthält hierzu die Maßnahmen 8.25 bis 8.29.*		
Frage 15: Verfügt Ihre Organisation bzw Ihr Unternehmen über ein Backup-, Redundanz- und Wiederherstellungsmanagement? ***Anmerkung:*** *Bei einem Datenverlust drohen der Organisation bzw dem Unternehmen schwerwiegende Verluste, weil dann idR die Geschäftsprozesse nicht oder nur teilweise funktionieren. Im Rahmen einer Backup-Strategie ist der Prozess zur Datensicherung zu definieren und zu dokumentieren. Es ist festzulegen, was, wie oft und wo Daten gesichert werden, verbunden mit der Festlegung entsprechender Integritäts- und Rücksicherungstests. Im Redundanzmanagement wird festgelegt, welche Systeme und Werkzeuge redundant ausgelegt werden, um im Falle eines Ausfalls reibungslose Abläufe zu gewährleisten. Im Wiederherstellungsplan (Disaster Recovery Plan) werden Handlungsweisen festgelegt, um den Betrieb wiederherzustellen.* *Das österreichische Informationssicherheitshandbuch setzt sich in Pkt 12.4 „Datensicherung“ mit diesem Thema sehr eingehend auseinander. Die ISO/IEC 27002 führt hierzu die Maßnahmen 8.13 und 8.14 an.*		
Frage 16: Verfügt Ihre Organisation bzw Ihr Unternehmen über Prozesse, die die Sicherheit bei der Beschaffung von IKT-Diensten und IKT-Produkten gewährleisten? ***Anmerkung:*** *Die Organisation bzw das Unternehmen sollte eine Richtlinie für die Lieferantenbeziehungen erstellen, wie die Lieferanten entsprechend der Sensibilität von Informationen, Produkten und Dienstleistungen zu bewerten und auszuwählen sind. Dabei ist zu berücksichtigen, wie der jeweilige Lieferant (wie zB IKT-Dienstleister, Logistik, Versorgungseinrichtungen, IKT-Infrastrukturkomponenten), die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen beeinträchtigen kann.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 15 „Lieferantenbeziehungen“ detaillierte Informationen zum Thema „Outsourcing“. Die ISO/IEC 27002 setzt sich mit den Maßnahmen 5.19 bis 5.23 sehr eingehend mit den Lieferantenbeziehungen auseinander.*		
Frage 17: Verfügt Ihre Organisation bzw Ihr Unternehmen über Prozesse, die eine sichere SW-Entwicklung gewährleisten? ***Anmerkung:*** *Bereits bei Vorliegen der Anwenderanforderungen sollte eine Risikoanalyse durchgeführt werden, deren Ergebnisse die Grundlage für die Formulierung der Anforderungen an die IT-Sicherheit bilden. Bei den Sicherheitsanforderungen sollten bei der Software-Entwicklung die Ausführungen der „Information Technology Security Evaluation Criteria“ (ITSEC) Berücksichtigung finden.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 14.1 detaillierte Informationen zum Thema „sichere SW-Entwicklung“. Die ISO/IEC 27002 setzt sich mit den Maßnahmen 8.25 bis 8.34 intensiv mit dieser Anforderung auseinander.*		
Frage 18: Trifft Ihre Organisation bzw Ihr Unternehmen geeignete Maßnahmen im Bereich der Netzwerksicherheit? ***Anmerkung:*** *Netzwerksicherheit umfasst alle Maßnahmen, die getroffen werden, um die Integrität des Computernetzwerks und der darin enthaltenen Daten zu gewährleisten. Durch entsprechende Sicherheitsstrategien und durch den Einsatz von diversen Security-Produkten können die Daten vor Cyberangriffen geschützt werden. Durch die Netzwerksegmentierung (Aufteilung des Netzwerks in Sicherheitsgrenzen) können Sicherheit und Leistung des Netzwerks erheblich verbessert werden.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 13.1 „Netzsicherheit“ ausführliche Informationen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahmen 8.20 bis 8.22 an.*		
Frage 19: Verfügt Ihre Organisation bzw Ihr Unternehmen über eine Kryptographie-Richtlinie? ***Anmerkung:*** *Zweck einer Kryptographie-Richtlinie ist die Festlegung von Regeln für die Anwendung kryptographischer Maßnahmen sowie der Regeln für die Nutzung kryptographischer Schlüssel, um die Vertraulichkeit, Integrität und Authentizität von Informationen zu schützen. Während es die Aufgabe der Informationsinhaber ist, die Informationen nach den Grundsätzen Vertraulichkeit, Integrität und Authentizität zu klassifizieren, liegt die technische Umsetzung im Bereich der IT.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 10 auf Basis der BSI-IT-Grundschutzbausteine[11] umfangreiche Informationen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahme 8.24 an.*		
Frage 20: Verfügt Ihre Organisation bzw Ihr Unternehmen über ein Betriebskontinuitäts- und Krisenmanagement? ***Anmerkung:*** *Durch das Betriebskontinuitätsmanagement soll die Verfügbarkeit der Information und der damit verbundenen Werte der Organisation bzw des Unternehmens während einer Störung (zB Cyberangriff) sichergestellt werden. Die Anforderungen an die IKT-Kontinuität ist das Ergebnis einer vorab durchgeführten Business-Impact-Analyse (BIA), im Rahmen derer die für die Organisation bzw das Unternehmen kritischen Geschäftsprozesse und Ressourcen sowie die notwendige Wiederanlaufzeit nach einem Störungsfall ermittelt werden, verbunden mit einer Risikobeurteilung. Im Rahmen des Krisenmanagements ist die Prüfung und die Behandlung von Sicherheitsvorfällen (Information Security Incident Management) zu regeln.* *Das österreichische Informationssicherheitshandbuch enthält in Pkt 17 „Disaster Recovery und Business Continuity“ ausführliche Informationen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahme 5.30 an.*		
Frage 21: Trifft Ihre Organisation bzw Ihr Unternehmen ausreichende Maßnahmen im Bereich der physischen und umgebungsbezogenen Sicherheit? *Anmerkung: Durch die Organisation bzw das Unternehmen ist der physische Schutz von Gebäuden gegen Brand, Wassereinbruch, Stromausfall, elektrische und elektromagnetische Risken, unbefugte Zutritte, Einbruch, Vandalismus usw sowie der entsprechenden Einrichtungen sicherzustellen.* *Das österreichische Informationssicherheitshandbuch enthält unter Pkt 11 „Physische und umgebungsbezogene Sicherheit“ detaillierte Ausführungen zu diesem Thema. Die ISO/IEC 27002 führt hierzu die Maßnahmen 7.1 bis 7.12 an.*		

[11] https://kurzlinks.de/ck9h.

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG. E-Mail: hj.pollirer@secur-data.at

Literatur und Links

- Österreichisches Informationssicherheitshandbuch, Version 4.4.0, Stand 6. 11. 2023;
- Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022, korrigierte Fassung 2022–03);
- Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024), Stand 24. 6. 2024 (nicht beschlossen);
- *WKO*, Die Leitungsorgane im Sinne der NIS-Gesetzgebung; www.wko.at/it-sicherheit/leitungsorgane-im-sinne-der-nis-gesetzgebung;
- *WKO*, Cybersicherheits-Richtlinie NIS 2; www.wko.at/it-sicherheit/nis2-uebersicht;
- *Security Insider*, In zehn Schritten zur NIS-2-Konformität; https://kurzlinks.de/3xk5;
- *WKO*, Online-Ratgeber: Cybersicherheitsrichtlinie – NIS2; https://ratgeber.wko.at/nis2/.

Viktoria Haidinger
Wirtschaftskammer Österreich

Michael Löffler
privacy awareness e.U.

Rechtsprechung

Datenübertragbarkeit. Kein Anspruch auf Datenübertragbarkeit bei Einstellung des Synchronisationsdiensts einer Fitness-App mangels Verantwortlicheneigenschaft.

Entscheidung

Die Betroffene nutzte seit 2017 einen Account bei der Anbieterin in Bezug auf eine Gesundheits- und Fitness-App und steht somit seit diesem Datum in einer auf den AGB basierenden Vertragsbeziehung mit dieser. Die Anbieterin stellte die App 2020 ein. Ab diesem Zeitpunkt fand keine Synchronisation der aufgezeichneten Daten mehr mit den Servern der Anbieterin statt, sondern die Trainingsdaten waren nur mehr lokal auf dem Mobiltelefon der Betroffenen gespeichert. Diese nutzte die App bis 2021. Die Betroffene beantragte die Übertragung ihrer Aktivitätsdaten ab dem Jahr 2020 durch die Anbieterin und die Zurverfügungstellung aller Aktivitätsdaten seit dem Jahr 2017 in einem strukturierten, gängigen und maschinenlesbaren Format. Auf der Homepage der Anbieterin kann eine betroffene Person die verarbeiteten Aktivitätsdaten abrufen und herunterladen. Die Betroffene hat von dieser Möglichkeit Gebrauch gemacht und eine Datenkopie ihrer eigenen Daten, die bei der Anbieterin auf deren Servern verarbeitet wurden, im JSON- bzw GPX-Format erhalten. Hochgeladene Fotos wurden im Export als JPEG oder GIF wiedergegeben. Die Dateiformate JSON und GPX können mit einfachen Mitteln und geringem Zeitaufwand auf einem Computer mit der Hilfe der vorinstallierten Anwendung „Editor“ und der kostenlosen Webapplikation Google Maps geöffnet und dargestellt werden.

Zwar wurden die Daten der Betroffenen lokal auf ihrem Endgerät von der App der Anbieterin verarbeitet, dies ist jedoch kein Hinweis darauf, dass die Anbieterin eine datenschutzrechtliche Verarbeitung vorgenommen hat: Die App war auf dem internen Speicher des Endgeräts der Betroffenen installiert und nahm ab dem Jahr 2020 keine Kommunikation zu den Servern oder anderen Kanälen der Anbieterin (mehr) vor. Die Betroffene verarbeitete sohin ihre eigenen Daten auf ihrem eigenen Endgerät und bediente sich dazu eines Tools, das die durch sie gesammelten Datenpunkte auf einer grafischen Oberfläche darstellte.

Sofern sich das Vorbringen der Betroffenen auf eine zivilrechtliche Vereinbarung mit der Anbieterin stützt, geht es ins Leere, da im verwaltungsbehördlichen Verfahren vor der DSB mit einer Beschwerde gem § 24 Abs 1 DSG nur die Verarbeitung von personenbezogenen Daten entgegen den Bestimmungen der DSGVO, § 1 oder Art 2 1. Hauptstück DSG durch eine:n Verantwortliche:n bekämpft werden kann. Eine womöglich zivilrechtliche Verpflichtung zur Verarbeitung von personenbezogenen Daten bzw Erbringung einer vereinbarten Leistung fällt in die Zuständigkeit der ordentlichen Gerichte. Der DSB ist außerdem in ihrer Einschätzung aus dem angefochtenen Bescheid recht zu geben, dass es für die Frage, ob eine datenschutzrechtliche Verarbeitung vorgenommen wurde, keine Rolle spielt, ob eine solche aus vertraglichen Verpflichtungen heraus vorgenommen werden hätte müssen.

Die DSB kam daher zu Recht zum Ergebnis, dass mangels einer Verarbeitung der personenbezogenen Daten der Betroffenen durch die Verantwortliche im Zeitraum von 2020 bis 2021 die Voraussetzungen für eine Verpflichtung der Verantwortlichen zur Datenübertragung iSd Art 20 DSGVO nicht gegeben sind.

Soweit für den Zeitraum davor das konkrete Format der Datenübertragung in Zweifel gezogen wird, ist darauf hinzuweisen, dass die Betroffene kein subjektives Recht auf die Wahl eines bestimmten Dateiformats hat. Das Format muss lediglich dem Zweck des Art 20 DSGVO entsprechen, was gegenständlich auch der Fall ist.