// KI-Hub VON STRUKTURAFLOW

FÖRDERUNG

DSGVO schützt Daten. NIS2 entscheidet, ob Ihr Betrieb einen Angriff übersteht

NIS2 ist kein Datenschutzgesetz. Wer Cybersicherheit wie DSGVO behandelt, ist im Ernstfall ungeschützt. Was das NISG 2026 für österreichische KMU bedeutet.

AUTOR
Natascha Reiner

VERÖFFENTLICHT
14. Mai 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/dsgvo-schuetzt-daten-nis2-entscheidet-ob-ihr-betrieb-einen-angriff-uebersteht/

NIS2 und DSGVO: Warum viele KMU gerade auf das falsche Problem vorbereiten

Montagmorgen, 7 Uhr. Die Systeme sind verschlüsselt. Produktion steht, Kommunikation ausgefallen, Kundendaten nicht erreichbar. Für viele Unternehmen klingt das nach Katastrophenszenario – dabei ist es längst Alltag geworden. IT-Sicherheit ist keine Kür mehr, sondern operative Notwendigkeit.

Trotzdem läuft gerade in vielen österreichischen KMU ein gefährliches Muster ab: NIS2 steht vor der Tür, die Geschäftsführung setzt ein Projektteam ein, kauft ein Dokumentationstool und hakt Schulungen ab. Fertig. Das Problem: Diese Unternehmen bereiten sich auf DSGVO 2.0 vor – dabei verlangt NIS2 etwas völlig anderes.

Dieser Artikel erklärt, warum der DSGVO-Reflex bei NIS2 schadet, was das österreichische NISG 2026 konkret bedeutet und welche drei Schritte Sie jetzt gehen sollten.

Zwei Gesetze, zwei Schutzlogiken: Der entscheidende Unterschied

NIS2 und DSGVO werden regelmäßig verwechselt. Das ist nachvollziehbar – beide drehen sich um IT-Systeme, beide haben mit Sicherheit zu tun, beide drohen mit empfindlichen Strafen. Trotzdem schützen sie grundverschiedene Dinge.

Die DSGVO schützt personenbezogene Daten. Wer darf sie verarbeiten, wie lange, mit welcher Rechtsgrundlage. Das Schutzziel ist der Mensch hinter den Daten. Die DSGVO ist ein Dokumentationsregime: Einwilligungen, Verarbeitungsverzeichnisse, Auftragsverarbeitungsverträge. Wer gut dokumentiert hat, gilt als compliant – unabhängig davon, ob seine Systeme sicher sind.

NIS2 schützt die Betriebsfähigkeit unter Angriff. Das Schutzziel ist nicht die Datei – es ist der laufende Betrieb. Die Produktion. Die Kommunikation. Die Lieferkette. Die Abrechnung. Alles, was aufhört zu funktionieren, wenn ein Angreifer erst einmal drin ist.

NIS2 fragt nicht, was im Ordner steht. Es fragt, was passiert, wenn Ihre Systeme um 3 Uhr morgens ausfallen. Ob Ihre Backups funktionieren. Ob Ihr Team weiß, wen es anruft. Ob Ihr Notfallplan je geprobt wurde.

Das ist ein Paradigmenwechsel: NIS2 optimiert auf Resilienz, nicht auf Nachweisbarkeit.

Was das in Österreich konkret bedeutet: NISG 2026

Österreich hat die NIS-2-Richtlinie der EU mit erheblicher Verspätung umgesetzt. Der erste Anlauf scheiterte 2024 im Nationalrat. Am 12. Dezember 2025 wurde das **Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026)** beschlossen und am 23. Dezember 2025 im Bundesgesetzblatt (BGBl. I Nr. 94/2025) kundgemacht.

Die wichtigsten Eckdaten

Ab 1. Oktober 2026 tritt das NISG 2026 in Kraft. Ab diesem Datum gelten alle Risikomanagementpflichten und Meldepflichten bei Sicherheitsvorfällen. Das bisherige NISG 2018 tritt gleichzeitig außer Kraft.

Bis 31. Dezember 2026 müssen sich betroffene Einrichtungen bei der neu geschaffenen Cybersicherheitsbehörde registrieren.

Bis September 2027 ist eine Selbstdeklaration zu den umgesetzten Sicherheitsmaßnahmen einzureichen.

Wer ist betroffen?

Mittlere und große Unternehmen ab 50 Mitarbeitenden oder über 10 Mio. Euro Jahresumsatz in einem der 18 definierten Sektoren – von Energie und Gesundheit über digitale Infrastruktur bis hin zu Lebensmittelproduktion und verarbeitendem Gewerbe.

Auch kleinere Unternehmen können über die Lieferkette in den Anwendungsbereich geraten: Wenn Sie ein größeres Unternehmen beliefern, das selbst NIS2-pflichtig ist, werden bestimmte Sicherheitsstandards vertraglich an Sie weitergegeben.

Strafen und Haftung

Verstöße können mit bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes geahndet werden.

Neu und entscheidend: Das NISG 2026 verankert erstmals eine **persönliche Haftung der Leitungsorgane** für Cybersicherheit – inklusive Schulungspflicht. Cybersicherheit ist damit keine IT-Angelegenheit mehr. Sie ist Chefsache.

Warum der DSGVO-Reflex bei NIS2 schadet

In vielen Unternehmen läuft gerade folgendes Muster ab: NIS2 landet auf dem Tisch, das Projektteam setzt sich zusammen, beginnt mit der Dokumentation, kauft ein Compliance-Tool und hakt Schulungen ab. Fertig.

Das ist der DSGVO-Reflex. Und er ist bei NIS2 gefährlich. Ähnliche Compliance-Fehler passieren beim EU AI Act, wo KMU ebenfalls operative Wirksamkeit statt nur Dokumentation brauchen.

NIS2 fragt nach Wirksamkeit, nicht nach Papier. Ein dokumentiertes Backup-Konzept, das nie getestet wurde, besteht keine NIS2-Prüfung – und hilft im Ernstfall noch weniger. Ein Notfallplan, den niemand kennt, ist kein Notfallplan.

Typische Schwachstellen, die dokumentiert ignoriert werden

- Vergessene Administratorkonten mit Standardpasswörtern (ein Einfallstor für Prompt Injection bei KI-Agenten)
- Fehlende Mehrfachauthentifizierung bei kritischen Systemen
- Zu breite Zugriffsrechte („Jeder kann alles sehen")
- Backups, die zwar laufen, aber nie wiederhergestellt wurden
- Notfallpläne ohne Kontaktdaten oder mit veralteten Zuständigkeiten

Diese Schwachstellen sind nicht durch Dokumentation zu schließen. Sie müssen technisch behoben und operational verankert sein.

Was Ihr Unternehmen jetzt braucht

Die verbleibende Zeit bis zum 1. Oktober 2026 ist keine Frist zum Abwarten. Sie ist eine Übergangsfrist zur Umsetzung. Der Unterschied ist erheblich.

Drei pragmatische Schritte zum Einstieg

1. Betroffenheit klären

Die WKO stellt einen Online-Ratgeber zur Verfügung, um eine erste Einschätzung vorzunehmen. Prüfen Sie auch indirekte Betroffenheit über die Lieferkette: Welche Ihrer Kunden sind NIS2-pflichtig? Welche Anforderungen werden sie an Sie stellen?

2. Gap-Analyse durchführen

- Welche kritischen Geschäftsprozesse hängen an IT-Systemen?
- Wo sind realistische Angriffswege? (Fernzugriffe, E-Mail, veraltete Software)
- Welche Kontrollen existieren bereits – und funktionieren sie nachweislich?
- Wann wurde das letzte Mal ein Backup wirklich wiederhergestellt?

3. Verantwortlichkeiten klären, bevor Tools gekauft werden

NIS2 braucht eine klare Ownership auf Leitungsebene. Diese Fragen sind vor jeder technischen Maßnahme zu beantworten:

- Wer ist im Ernstfall zuständig?
- Wer entscheidet über die Meldung eines Vorfalls?
- Wer kommuniziert mit der Cybersicherheitsbehörde?
- Wer koordiniert die Wiederherstellung?

Strukturaflow unterstützt KMU im DACH-Raum dabei, diesen Prozess strukturiert – nicht hektisch – anzugehen. Von der ersten Betroffenheitsanalyse bis zur operativen Umsetzung von Risikomanagementmaßnahmen.

Förderung nicht vergessen: KMU.DIGITAL

Viele österreichische Unternehmen wissen nicht, dass NIS2-Umsetzungsprojekte förderfähig sein können. Über das Förderprogramm **KMU.DIGITAL** des Bundesministeriums für Arbeit und Wirtschaft werden Digitalisierungs- und IT-Sicherheitsprojekte für kleine und mittlere Unternehmen finanziell unterstützt.

Das bedeutet: Der Weg zur NIS2-Konformität muss nicht vollständig aus eigener Tasche finanziert werden. Förderfähig sind typischerweise:

- Externe Beratung zur Risikoanalyse und Gap-Analyse (ähnlich einem KI-Audit für KMU)
- Implementierung technischer Sicherheitsmaßnahmen
- Mitarbeiterschulungen zu Cybersicherheit
- Penetrationstests und Security-Audits

Ob Ihr Unternehmen förderberechtigt ist und welche Maßnahmen abgedeckt werden können, sollten Sie frühzeitig klären. Einen detaillierten Überblick über Förderoptionen für österreichische KMU finden Sie in unserem Leitfaden: KI Förderung Österreich 2026.

Nächste Schritte

DSGVO und NIS2 verfolgen unterschiedliche Ziele mit unterschiedlichen Mitteln. Während die DSGVO bei ChatGPT im Unternehmen primär den Datenschutz regelt, zielt NIS2 auf Betriebssicherheit ab. Wer beides in einen Topf wirft, unterschätzt NIS2 systematisch. Die Richtlinie verlangt keine perfekte Dokumentation. Sie verlangt einen Betrieb, der einen Angriff übersteht.

Das NISG 2026 gibt österreichischen Unternehmen bis Oktober 2026 Zeit zur Umsetzung. Das ist keine Entwarnung – es ist ein Startschuss.

Kostenloses Erstgespräch mit Strukturaflow

In 30 Minuten besprechen wir Ihre Ausgangssituation, klären die Betroffenheit nach NISG 2026 und zeigen Ihnen, welche nächsten Schritte sinnvoll sind – inklusive möglicher Förderoptionen.

→ Erstgespräch buchen

Natascha Reiner ist Gründerin und CEO von Strukturaflow IT-Systemhaus in Fohnsdorf (Steiermark). Strukturaflow begleitet KMU im DACH-Raum bei Prozessautomatisierung, Corporate AI und IT-Infrastruktur.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com