7408/J
vom 22.10.2026 (XXVIII. GP)

Anfrage

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

an den Bundesminister für Finanzen

betreffend Umsetzung des Netz- und Informationssystemsicherheitsgesetzes 2026 im Ressort

BEGRÜNDUNG

Am 1. Oktober 2026 ist das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) in Kraft getreten, mit dem Österreich die europäische NIS-2-Richtlinie umsetzt. Seit diesem Tag gelten die Meldepflichten für erhebliche Cybersicherheitsvorfälle. Wesentliche und wichtige Einrichtungen müssen sich binnen drei Monaten, also bis 31. Dezember 2026, registrieren. Bis 1. Oktober 2027 ist eine Selbstdeklaration zu den umgesetzten Risikomanagement-Maßnahmen vorzulegen, die Maßnahmen sind dabei bereits jetzt zu ergreifen und haben zumindest die in § 32 Abs 4 NISG 2026 angeführten Inhalte zu umfassen. Ab 1. Oktober 2028 kann die Behörde prüfen.[1] Das Gesetz erfasst nicht nur Unternehmen, sondern auch Einrichtungen der öffentlichen Verwaltung.[2]

Von tausenden Unternehmen verlangt der Staat damit ein wirksames Risikomanagement, geschulte Leitungsorgane, gesicherte Lieferketten und funktionierende Meldeprozesse. Glaubwürdig ist das nur, wenn die Bundesverwaltung dieselben Anforderungen selbst erfüllt. Die Ministerien verwalten die sensibelsten Daten der Republik und sind regelmäßig Ziel von Cyberangriffen. Die Zahl der Cyberangriffe in Österreich ist im Jahr 2025 erneut gestiegen.[3]

Die Anfrageserie der unterfertigenden Abgeordneten zu Cybersicherheitsvorfällen in den Bundesministerien vom 27. März 2026 hat gezeigt, dass auch die Ressorts selbst betroffen sind. Gleichzeitig hat die Bundesregierung beschlossen, bis 2029 sechs Prozent des Verwaltungsdienstes nicht nachzubesetzen. Wie das mit dem zusätzlichen Personalbedarf für Informationssicherheit vereinbar ist, ist offen.

Zum Start des NISG 2026 soll daher erhoben werden, wie gut die einzelnen Ressorts vorbereitet sind, welche Einrichtungen unter das Gesetz fallen und ob die Registrierung bis Jahresende gelingt.

---

[1] digital-recht.at, Die Fristen nach dem österreichischen NISG 2026, 23.2.2026, https://www.digital-recht.at/blog/die-fristen-nach-dem-osterreichischen-nisg-2026---alle-wichtigen-termine-im-uberblick
[2] Parlament, NISG 2026, https://www.parlament.gv.at/gegenstand/XXVIII/BNR/126
[3] Anfrage 5488/J XXVIII. GP vom 27.3.2026 mit Verweis auf den Cyber Security Report 2025, https://www.parlament.gv.at/dokument/XXVIII/J/5488/imfname_1748508.pdf

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Welche Einrichtungen im Wirkungsbereich Ihres Ressorts fallen unter das NISG 2026? (Aufschlüsselung nach Zentralstelle, nachgeordneten Dienststellen, ausgegliederten Rechtsträgern und Beteiligungen sowie nach wesentlichen und wichtigen Einrichtungen)
2) Wurden diese Einrichtungen bereits registriert?
   a. Wenn ja, wann?
   b. Wenn nein, bis wann ist die Registrierung geplant?
3) Welche Funktion bzw. Organisationseinheit ist in Ihrem Ressort für die Umsetzung des NISG 2026 verantwortlich, und wer ist Ansprechstelle gegenüber der Cybersicherheitsbehörde?
4) Wurde vor dem Inkrafttreten eine Gap-Analyse oder ein Audit zur NISG-Konformität durchgeführt?
   a. Wenn ja, durch wen und mit welchem Ergebnis?
   b. Welche Kosten sind dafür entstanden?
   c. Wenn nein, warum nicht?
5) Wie ist der Stand der Umsetzung der Risikomanagementmaßnahmen nach dem NISG 2026? (Aufschlüsselung nach Inhalten gem § 32 Abs 4, insbes Risikoanalyse, Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebs und Krisenmanagement, Sicherheit der Lieferkette, Sicherheitsmaßnahmen und Schwachstellenmanagement, Kryptografie, Zugriffskontrolle, Multi-Faktor-Authentifizierung und Schulungen)
6) Sind die Meldeprozesse für erhebliche Sicherheitsvorfälle (Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht) eingerichtet?
   a. Wurden sie in einer Übung erprobt? Wenn ja, wann?
7) Wie viele erhebliche Cybersicherheitsvorfälle wurden seit 1. Oktober 2026 von Einrichtungen Ihres Ressorts gemeldet? (Aufschlüsselung nach Art des Vorfalls)
8) Wurden die Leitungsorgane Ihres Ressorts zu Cybersicherheit geschult?
   a. Wenn ja, wie viele Personen in welchem Umfang?
   b. Wenn nein, bis wann ist das geplant?
9) Wie viele Bedienstete Ihres Ressorts haben in den Jahren 2025 und 2026 Schulungen zu Cybersicherheit absolviert?
10) Wurde die Sicherheit der Lieferkette bewertet?
   a. Welche IT-Dienstleister werden als kritisch eingestuft?
   b. Wie viele davon haben ihren Sitz außerhalb der EU?
   c. Wurden bestehende Verträge mit IT-Dienstleistern, einschließlich des Bundesrechenzentrums, an die Anforderungen des NISG 2026 angepasst?

11) Wie viele Vollbeschäftigungsäquivalente sind in Ihrem Ressort in den Bereichen IT und Informationssicherheit tätig? (Aufschlüsselung nach den Jahren 2024, 2025 und 2026 sowie nach besetzten und unbesetzten Planstellen)

12) Welcher zusätzliche Personalbedarf ergibt sich aus dem NISG 2026 für Ihr Ressort?
   a. Wie wird dieser Bedarf mit der beschlossenen Nichtnachbesetzung im Verwaltungsdienst vereinbart?
   b. Sind Planstellen im Bereich IT und Informationssicherheit von der Nichtnachbesetzung ausgenommen?

13) Welche Budgetmittel sind für die Umsetzung des NISG 2026 in den Jahren 2026 und 2027 vorgesehen, und welche Kosten sind bisher angefallen? (Aufschlüsselung nach Personal, Technik und externer Beratung)

14) Wie wurden die Erkenntnisse aus den Cybersicherheitsvorfällen, die Ihr Ressort in der Beantwortung der Anfrage vom 27. März 2026 angegeben hat, in der Umsetzung des NISG 2026 berücksichtigt?

15) Bestehen für alle kritischen Systeme vom Netz getrennte Sicherungskopien?
   a. Wann wurde die Wiederherstellung zuletzt getestet?

16) Wie hoch ist der Anteil der Zugänge zu IT-Systemen Ihres Ressorts, die mit Multi-Faktor-Authentifizierung abgesichert sind?

17) Welche weiteren Maßnahmen setzt Ihr Ressort bis zur Selbstdeklaration am 1. Oktober 2027, und nach welchem Zeitplan?

18) Werden die Standards des NISG 2026 auch in Einrichtungen Ihres Ressorts angewendet, die nicht unter das Gesetz fallen?
   a. Wenn nein, warum nicht?

19) Wurde bei der Beantwortung dieser Anfrage Künstliche Intelligenz eingesetzt?
   a. Wenn ja, welche Anwendung und in welchen Arbeitsschritten?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-10-22T12:15:17+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	