2654/AB
vom 10.10.2025 zu 3136/J (XXVIII. GP)

Bundesministerium
Wirtschaft, Energie
und Tourismus

bmwet.gv.at

Dr. Wolfgang Hattmannsdorfer
Bundesminister

Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.647.467

Ihr Zeichen: BKA - PDion (PDion)3136/J-NR/2025

Wien, am 10. Oktober 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba und weitere haben am 12.08.2025 unter der **Nr. 3136/J** an mich eine schriftliche parlamentarische Anfrage betreffend **IT- und Cybersicherheit im Bundesministerium für Wirtschaft, Energie und Tourismus sowie bei Mitarbeiter:innen in Schlüsselpositionen** gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 und 2

- *Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter: innen?*
- *Gibt es gesonderte Vorgaben für den Umgang mit vertraulichen Informationen auf mobilen Geräten, insbesondere hinsichtlich Verschlüsselung, Zwei Faktor Authentifizierung und Speicherung sensibler Daten?*

Die für das Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET) ressortweit erlassene Informationssicherheitsrichtlinie sowie die IKT-Nutzungsverordnung bilden die Basis für den sorgsamen und sicheren Umgang mit Informationen und eingesetzten IKT-Systemen. In der gesonderten IKT-Nutzungsrichtlinie werden konkrete Details hinsichtlich der Handhabe mit dienstlichem IKT-Equipment geregelt. Für spezielle Situationen

oder Tätigkeiten, wie etwa Dienstreisen oder vertrauliche Informationen in IKT-Services, existieren weitere Vorgaben im Hinblick auf die Informationssicherheit.

Zur Frage 3

- *In welchen zeitlichen Abständen werden Sicherheitsüberprüfungen oder Audits der dienstlichen IT Geräte durchgeführt, sowohl im Inland als auch bei im Ausland tätigen Mitarbeiter:innen?*
    - *Wie oft finden diese Audits im Durchschnitt pro Jahr statt?*
    - *Welche internen oder externen Stellen führen diese Audits durch?*

Die IKT-Infrastruktur des BMWET wird regelmäßig einem gesamtheitlichen Audit unterzogen. Darüber hinaus gibt es mehrere teils hochzyklische Prüfungen von einzelnen Komponenten oder Bereichen. Das gesamtheitliche Audit wird von einem externen Cybersecurity-Dienstleister durchgeführt. Um die Objektivität zu wahren, werden dafür alternierend unterschiedliche Dienstleister eingesetzt.

Zur Frage 4

- *Werden Diensthandys oder andere mobile Geräte auf Reisen in Länder mit erhöhtem Spionagerisiko durch „Burner Phones" oder andere Einweggeräte ersetzt?*
    - *Wenn ja, seit wann gilt diese Praxis und für welche Destinationen?*

In den in der Antwort zu den Fragen 1 und 2 genannten internen Richtlinien ist vorgesehen, dass dienstliches IKT-Equipment in bestimmte Länder nicht mitgeführt werden darf. Bei Bedarf werden in solchen Fällen Einweggeräte zur Verfügung gestellt.

Zur Frage 5

- *Welche Maßnahmen bestehen, um das Risiko der Nutzung unsicherer öffentlicher Netzwerke (z. B. Hotel WLANs) durch Mitarbeiter:innen zu minimieren?*

Gemäß den in der Antwort zu den Fragen 1 und 2 genannten internen Richtlinien ist primär der Hotspot am eigenen Dienst-Smartphone zu verwenden. Die automatische Verschlüsselung der Verbindungsinformationen trägt zusätzlich zur Risikominimierung bei.

Zur Frage 6

- *Wie werden die Mitarbeiter:innen in Fragen der IT Sicherheit geschult?*
    - *Gibt es verpflichtende Schulungen für alle Beschäftigten?*
    - *In welchen zeitlichen Abständen werden diese Schulungen angeboten?*

- *Werden Sondertrainings für besonders exponierte Funktionen oder Mitarbeiter:innen in Schlüsselpositionen durchgeführt?*

Allen Bediensteten des BMWET werden ein eigens konzipiertes e-Learning sowie eine an mehreren Terminen pro Jahr zur Verfügung gestellte intensive Präsenzschulung, angepasst an die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen, angeboten. Diese Schulungen sind im Zuge der Grundausbildung verpflichtend zu absolvieren. Zusätzlich besteht die Möglichkeit, an Schulungsmaßnahmen aus dem Bildungsprogramm der Verwaltungsakademie des Bundes teilzunehmen. In Hinblick auf die erwartete nationale Umsetzung der EU-NIS2-Richtlinie werden Sondertrainings im Sinne der Anfrage angedacht.

Zur Frage 7

- *Welche Abteilungen oder Teams sind innerhalb Ihres Hauses für IT Sicherheit und Cyberabwehr zuständig?*
  - *Wie viele Planstellen sind aktuell für diesen Bereich vorgesehen?*
  - *Wie viele davon sind mit qualifiziertem Personal besetzt?*

Dazu ist auf die Beantwortung der parlamentarischen Anfrage Nr. 561/J zu verweisen.

Zur Frage 8

- *Wie hoch war das jährliche Budget Ihres Ressorts für IT- und Cybersicherheit in den letzten fünf Jahren (bitte nach Jahren aufschlüsseln)?*

Aufgrund unterschiedlicher Vertrags-, Dienstleistungs- und Verrechnungsmodalitäten wie etwa einer Mischung aus Pauschalen und Abrechnung nach tatsächlichem Aufwand sowie der Tatsache, dass IT- und Cybersicherheit eine Querschnittsmaterie darstellt, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

Zur Frage 9

- *Gibt es eine regelmäßige Evaluierung der vorhandenen Sicherheitsstandards unter Einbeziehung externer Sicherheits- und Datenschutzexperten? Wenn ja, wann fand die letzte Evaluierung statt und welche Ergebnisse wurden daraus abgeleitet?*

Neben den in der Antwort zu Frage 3 erwähnten Überprüfungen und den daraus resultierenden Ergebnisberichten finden regelmäßig strategische Cybersecurity-Meetings mit dem IKT-Dienstleister des BMWET statt, um das engmaschige Netz an Maßnahmen weiter zu verbessern. Von einer Auflistung der Ergebnisse ist zum Erhalt des bestehenden hohen

IKT- Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz sowie im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand zu nehmen.

Zur Frage 10

- *Wurden nach Bekanntwerden des eingangs erwähnten Sicherheitsvorfalls im Jahr 2025 konkrete Maßnahmen gesetzt, um ähnliche Fälle künftig zu verhindern?*
    - *Wenn ja, welche?*

Die bestehenden technischen und organisatorischen Maßnahmen im Ressort wurden als angemessen eingestuft.

Zur Frage 11

- *Inwieweit arbeitet Ihr Haus mit nationalen und internationalen Stellen (z.B. DSN, CERT, EU Partner) zusammen, um sich über aktuelle Bedrohungen und Best Practices auszutauschen?*

Die relevanten Verantwortlichen im BMWET stehen in regelmäßigem Austausch mit ihren Pendants in den anderen Ressorts sowie zentralen Stellen wie der Direktion Staatsschutz und Nachrichtendienst oder CERT.at. Über diese Gremien wird auch der weitere internationale Austausch aufrechterhalten.

Zur Frage 12

- *Gibt es Meldewege oder Whistleblower Plattformen für Mitarbeiter: innen, um Sicherheitslücken oder ungewöhnliche Vorfälle anonym zu melden?*
    - *Wenn ja, wie wird sichergestellt, dass diese Hinweise unverzüglich bearbeitet werden?*

Den Mitarbeiterinnen und Mitarbeitern des BMWET stehen neben ihren jeweiligen Führungskräften die Informationssicherheitsbeauftragten gemäß § 7 Informationssicherheitsgesetz, die Datenschutzbeauftragten, die IKT-Abteilung, die Personalabteilung sowie die Rechtsabteilung beratend und unterstützend zur Seite. Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 bzw. § 5 Abs. 1 Vertragsbedienstetengesetz 1948 hingewiesen. Wird demnach einer oder einem Bundesbediensteten in Ausübung des Dienstes der begründete Verdacht einer von amtswegen zu verfolgenden gerichtlich strafbaren Handlung bekannt, die den Wirkungsbereich der Dienststelle betrifft, der sie oder er angehört, so ist dies unverzüglich der Leiterin oder dem Leiter der Dienststelle zu melden. Gemäß HinweisgeberInnenschutzgesetz können sich Hinweis-

geberinnen und Hinweisgeber bei Rechtsverletzungen außerdem – auf Wunsch auch anonym – an die zuständige interne Meldestelle wenden.

Dr. Wolfgang Hattmannsdorfer

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WIRTSCHAFT, ENERGIE UND TOURISMUS @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Wirtschaft, Energie und Tourismus
	Datum/Zeit	2025-10-10T08:32:17+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2082304761
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T08:37:36+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	