2665/AB
vom 10.10.2025 zu 3135/J (XXVIII. GP)

Bundesministerium
Innovation, Mobilität
und Infrastruktur

bmimi.gv.at

Peter Hanke
Bundesminister

ministerbuero@bmimi.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 W i e n

Geschäftszahl: 2025-0.646.128

10. Oktober 2025

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Zorba, Freundinnen und Freunde haben am 12. August 2025 unter der **Nr. 3135/J** eine schriftliche parlamentarische Anfrage betreffend IT- und Cybersicherheit im Bundesministerium für Innovation, Mobilität und Infrastruktur sowie bei Mitarbeiter:innen in Schlüsselpositionen an mich gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu Frage 1:

- *Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter:innen?*

Im Wesentlichen darf auf folgende Richtlinien hingewiesen werden:

- IKT-Nutzungsverordnung (IKT-NV), BGBl. II Nr. 281/2009
- IT-Sicherheitspolitik
- IKT-Arbeitsplatzrichtlinie
- diverse konkrete Handlungsempfehlungen (z.B. Sicherheit und mobiles Arbeiten oder Umgang mit IKT-Ausstattung bei Auslandsdienstreisen)

Das Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI) führt darüber hinaus eine permanente Lage- und Risikobeurteilung für Gefahren aus dem Cyber- und Informationsraum durch und stellt aktuelle und konkrete Anleitungen und Empfehlungen über die internen Kommunikationsmittel meines Ressorts zur Verfügung. Darüber hinaus findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt.

Zu den Fragen 2 bis 5 und 9 bis 11:

- *Gibt es gesonderte Vorgaben für den Umgang mit vertraulichen Informationen auf mobilen Geräten, insbesondere hinsichtlich Verschlüsselung, Zwei Faktor Authentifizierung und Speicherung sensibler Daten?*
- *In welchen zeitlichen Abständen werden Sicherheitsüberprüfungen oder Audits der dienstlichen IT Geräte durchgeführt, sowohl im Inland als auch bei im Ausland tätigen Mitarbeiter:innen?*
    a) *Wie oft finden diese Audits im Durchschnitt pro Jahr statt?*
    b) *Welche internen oder externen Stellen führen diese Audits durch?*
- *Werden Diensthandys oder andere mobile Geräte auf Reisen in Länder mit erhöhtem Spionagerisiko durch „Burner Phones" oder andere Einweggeräte ersetzt?*
    a) *Wenn ja, seit wann gilt diese Praxis und für welche Destinationen?*
- *Welche Maßnahmen bestehen, um das Risiko der Nutzung unsicherer öffentlicher Netzwerke (z.B. Hotel WLANs) durch Mitarbeiter:innen zu minimieren?*
- *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?*
- *Wurden nach Bekanntwerden des eingangs erwähnten Sicherheitsvorfalls im Jahr 2025 konkrete Maßnahmen gesetzt, um ähnliche Fälle künftig zu verhindern?*
    a) *Wenn ja, welche?*
- *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?*

Für mein Ressort hat der Schutz der verarbeiteten Daten sowie der eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Daher verfolgt mein Ministerium den Ansatz eines Informationssicherheitsmanagementsystems, das unter Berücksichtigung der datenschutzrechtlichen Anforderungen entwickelt wird und sich an internationalen Sicherheitsstandards orientiert.

Das Managementsystem soll unter anderem sicherstellen, dass die geltenden Rechtsvorschriften eingehalten werden und bestehende Risiken systematisch identifiziert, bewertet und durch geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des aktuellen Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden können. Es sieht darüber hinaus vor, dass die Aktualität der geltenden Regelungen sowie die Wirksamkeit der getroffenen Maßnahmen sowohl regelmäßig als auch im Anlassfall überprüft, bewertet und evaluiert wird. Dabei wird auch die Expertise externer Stellen eingebunden.

Die Evaluierung und Aktualisierung der entsprechenden Erlässe erfolgen fortlaufend. Die öffentlich verfügbaren Sicherheitsstandards dienen dabei als Grundlage und definieren umfassende Anforderungs- und Maßnahmenkataloge.

Gemäß den Länderbewertungen des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) und des Bundesministeriums für Inneres (BMI) bzw. der Direktion Staatsschutz und Nachrichtendienst (DSN) werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie zum Beispiel den Handlungsempfehlungen der DSN gesetzt.

Im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen, muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zu Frage 6:

- *Wie werden die Mitarbeiter:innen in Fragen der IT Sicherheit geschult?*
  - *a) Gibt es verpflichtende Schulungen für alle Beschäftigten?*
  - *b) In welchen zeitlichen Abständen werden diese Schulungen angeboten?*
  - *c) Werden Sondertrainings für besonders exponierte Funktionen oder Mitarbeiter:innen in Schlüsselpositionen durchgeführt?*

Es ist vorgesehen, in regelmäßigen Abständen verpflichtende Schulungen anzubieten und abzuhalten. Die Schulungen werden dabei auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen abgestimmt. Im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich angeboten.

Zu Frage 7:

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

Laut Geschäfts- und Personaleinteilung (GPE) ist die Abteilung Präsidium 4 – Informations- und Kommunikationstechnik zuständig.

Zu Frage 8:

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

Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

Zu Frage 12:

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

Der Leiter der Bundesdisziplinarbehörde ist für mein Ressort die interne Stelle für Meldungen von Hinweisgeber:innen gemäß HinweisgeberInnenschutzgesetz (§ 12 Abs. 1 Z 1 HSchG).

In Zusammenhang mit Cybersicherheit fallen Hinweise zur Verletzung von Vorschriften in den folgenden Bereichen in den sachlichen Geltungsbereich des HSchG: „Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen“ (§ 3 Abs. 3 Z 10 HSchG). Hinweisgeber:innen gemäß HSchG können hierzu Hinweise anonym bei dem:der Leiter:in der Bundesdisziplinarbehörde einbringen (https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=Dxuw3U&c=-1&language=ger).

Kontaktstelle für die interne Stelle im BMIMI ist der Leiter der Abteilung Interne Revision und EU-Finanzkontrolle. Wenn dieser einen Hinweis von der internen Stelle erhält, prüft er diesen umgehend auf seine Stichhaltigkeit und geht dem Hinweis ressortintern nach. Das Ergebnis der ressortinternen Prüfung wird der internen Stelle von dem Leiter der Abteilung Interne Revision und EU-Finanzkontrolle mitgeteilt.

Spätestens drei Monate nach Entgegennahme eines Hinweises hat die interne Stelle den:die Hinweisgeber:in über die bereits ergriffenen oder beabsichtigten Folgemaßnahmen zu informieren. Wenn ein Hinweis nicht weiterverfolgt wird, ist dies gegenüber dem:der Hinweisgeber:in zu begründen (§ 13 Abs. 9 HSchG).

Mit freundlichen Grüßen

Peter Hanke

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNOVATION, MOBILITÄT UND INFRASTRUKTUR @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2025-10-10T15:18:14+02:00
	Seriennummer	2069212815
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T15:19:40+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	