2650/AB
vom 09.10.2025 zu 3129/J (XXVIII. GP)

Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

sozialministerium.gv.at

Korinna Schumann
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2025-0.654.058

Wien, 1.10.2025

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 3129/J des Abgeordneten Süleyman Zorba betreffend IT- und Cybersicherheit im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz sowie bei Mitarbeiter:innen in Schlüsselpositionen** wie folgt:

Frage 1: *Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter: innen?*

Folgende Richtlinien bestehen derzeit im Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK):

- IKT-Nutzungsverordnung (IKT-NV), BGBl. II Nr. 281/2009 (Änderung BGBl. II Nr. 107/2018)
- IKT-Sicherheitspolitik des BMASGPK
- IKT-Benutzungsrichtlinien des BMASGPK
- Grundregeln der Informationssicherheit

Diese Richtlinien wurden als verbindliche Vorschriften im Ressort etabliert und werden in regelmäßigen Abständen aktualisiert. Außerdem gibt es laufend Schulungsmaßnahmen, verpflichtende e-learnings und andere Maßnahmen, die die Kompetenz der

Mitarbeiterinnen und Mitarbeiter zur Fragen der IT-Sicherheit auf einem hohen Maß halten sollen.

Darüber hinaus findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt. Aus den gemeinsamen Gremien wird eine permanente Lage- und Risikobeurteilung für Gefahren aus dem Cyber- und Informationsraum durchgeführt und aktuelle und konkrete Anleitungen sowie Empfehlungen zur Verfügung gestellt.

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 das BMASGPK hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten höchste Priorität. Das BMASGPK verfügt daher über ein Informationssicherheits- und Managementsystem, welches sich an internationalen Sicherheitsstandards orientiert.

Das Managementsystem sorgt unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden. 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 genutzt, wie z.B. von Computer-Notfallteams im Sinne des vierten Abschnitts des Netz- und Informationssystemsicherheitsgesetzes (NISG) und von qualifizierten Stellen im Sinne des § 3 Z 11 NISG.

Die IKT-Benutzungsrichtlinien des BMASGPK geben Handlungsanweisungen zu Schutzmaßnahmen auf Dienstreisen und zur Nutzung von ungesicherten WLAN-Netzwerken vor. Die Evaluierung und Aktualisierung der diesbezüglichen Rundschreiben erfolgen laufend. Die öffentlich verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

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?

Ja, im BMASGPK müssen alle Mitarbeiter:innen im Bereich IT-Sicherheit verpflichtende Schulungen durchführen, sowohl in Präsenz als auch online über E-Learnings. Die Schulungen werden auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Alle Mitarbeiter:innen sind z.B. verpflichtet, E-Learnings zum Thema IT-Sicherheit in periodischen Abständen zu absolvieren. Führungskräfte müssen zusätzlich an einem Seminar zur Umsetzung der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-2-RL) teilnehmen. Betreffend Absolvierung der E-Learnings finden regelmäßig Erhebungen über das Bildungscontrolling statt.

Zudem werden für die entsprechenden Bedienstetengruppen zu folgenden Themen weitere Schulungen, E-Learning-Programme und Lehrvideos angeboten, um die Mitarbeiter:innen für das Thema zu sensibilisieren und niederschwellig Informationsangebote bereitzustellen: Cyber Crime, Security Awareness Training, Phishing und Ransomware.

Ergänzend zum ressortinternen Angebot stehen allen Bediensteten im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes umfassende Aus-, Fort- und Weiterbildungsmaßnahmen zum Thema IT-Sicherheit zur Verfügung.

Darüber hinaus erfolgen laufend Informationen über die verschiedensten Informationskanäle (E-Mail, Intranet, Mitarbeiter:innen-Zeitung etc.).

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?

Für die „IT-Sicherheit und Cyberabwehr" sind die Abteilungen I/B/8 und VI/B/10 zuständig. Ergänzend wird auf die Geschäftseinteilung des BMASGPK hingewiesen, wobei die Mitarbeiter:innen mit unterschiedlichen Aufgaben betraut sind und eine genaue Zurechnung zur Informationssicherheit nicht möglich ist.

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 zuzuordnen.

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?

Ja, es gibt etablierte Meldewege und –plattformen für Mitarbeiter:innen über die Bundesdisziplinarbehörde. Die zuständigen Stellen bearbeiten die Meldungen unverzüglich und setzen die notwendigen Maßnahmen. Nicht anonymisierte Meldungen erfolgen an den IT-Support.

Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 (für Vertragsbedienstete iVm § 5 Abs. 1 Vertragsbedienstetengesetz 1948) hingewiesen. Wird demnach den Bundesbediensteten in Ausübung des Dienstes der

begründete Verdacht einer von Amts wegen zu verfolgender gerichtlich strafbarer Handlung bekannt, die den Wirkungsbereich der Dienststelle betrifft der sie bzw. er angehört, so ist dies unverzüglich dem Leiter der Dienststelle zu melden.

Gemäß Hinweisgeberinnenschutzgesetz können sich außerdem Hinweisgeber:innen, insbesondere Mitarbeitende des Ressorts, bei Rechtsverletzungen – auf Wunsch auch anonym – an die zuständige interne Meldestelle bzw. an die zuständige externe Meldestelle für das Ressort wenden. Eine rasche Bearbeitung der eingegangenen Meldungen wird über einen Single-Point-of-Contact im Ressort sichergestellt.

Auf der Homepage des BMASGPK wird für die Abgabe eines Hinweises auf die interne Meldestelle (Bundesdisziplinarbehörde) verwiesen/verlinkt.

Mit freundlichen Grüßen

Korinna Schumann

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2025-10-09T12:08:10+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.	1088205675
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-09T12:15:38+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	