2656/AB
vom 10.10.2025 zu 3128/J (XXVIII. GP)

Bundesministerium
Frauen, Wissenschaft
und Forschung

bmfwf.gv.at

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlamentsdirektion
Dr.-Karl-Renner-Ring 3
1017 Wien

Geschäftszahl: 2025-0.646.145

Die schriftliche parlamentarische Anfrage Nr. 3128/J-NR/2025 betreffend betr. IT- und Cybersicherheit im Bundesministerium für Frauen, Wissenschaft und Forschung sowie bei Mitarbeiter:innen in Schlüsselpositionen, die die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen am 12. August 2025 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

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,
- interne Benutzerrichtlinien (Richtlinien für Nutzung von Notebooks, Smartphones etc.),
- diverse konkrete Handlungsempfehlungen wie zum Beispiel für die „Sicherheit bei Onlinediensten“.

Das BMFWF 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 des BMFWF zur Verfügung. Zusätzlich findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt.

Zu den Fragen 2, 3, 4, 5, 9, 10 und 11:

2. Gibt es gesonderte Vorgaben für den Umgang mit vertraulichen Informationen auf mobilen Geräten, insbesondere hinsichtlich Verschlüsselung, Zwei Faktor Authentifizierung und Speicherung sensibler Daten?
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?
a) Wie oft finden diese Audits im Durchschnitt pro Jahr statt?
b) Welche internen oder externen Stellen führen diese Audits durch?
4. 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?
5. Welche Maßnahmen bestehen, um das Risiko der Nutzung unsicherer öffentlicher Netzwerke (z. B. Hotel WLANs) durch Mitarbeiter:innen zu minimieren?
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?
10. Wurden nach Bekanntwerden des eingangs erwähnten Sicherheitsvorfalls im Jahr 2025 konkrete Maßnahmen gesetzt, um ähnliche Fälle künftig zu verhindern?
a) Wenn ja, welche?
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?

Für das BMFWF hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das BMFWF orientiert sich in der Sicherheitsorganisation an internationalen Sicherheitsstandards.

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.

Gemäß BMEIA und BMI/DSN Länderbewertungen werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie z.B. den Handlungsempfehlungen der Direktion Staatsschutz und Nachrichtendienst gesetzt.

Zu Frage 6:

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 werden in regelmäßigen Abständen Schulungen und Awarenessprogramme angeboten und abgehalten. Die Schulungen werden auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich angeboten.

Zu Frage 7:

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?

Gemäß Geschäftseinteilung des BMFWF liegt die Zuständigkeit im Referat Präs/9c.

Da die Mitarbeiter:innen im Bereich der Informationssicherheit in einem sensiblen Bereich tätig sind, muss aus Gründen der Informationssicherheit und des Datenschutzes von einer Nennung weiterer Details Abstand genommen werden.

Zu Frage 8:

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:

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?

Es gibt etablierte Meldewege und -plattformen. Eine unverzügliche Behandlung wird durch das entsprechende interne Personal sowie über zugekaufte Sicherheitsdienstleistungen sichergestellt.

Den Mitarbeiter:innen des BMFWF stehen zusätzlich ihre Führungskräfte, der Informationssicherheitsbeauftragte gemäß § 7 Informationssicherheitsgesetz, der Datenschutzbeauftragte, die Personalabteilung sowie die Rechtsabteilung beratend und unterstützend zur Seite.

Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 (für Vertragsbedienstete iVm § 5 Abs. 1 Vertragsbedienstetengesetz 1948) hingewiesen. Wird demnach dem Bundesbediensteten in Ausübung des Dienstes der begründete Verdacht einer von Amts wegen zu

verfolgenden gerichtlich strafbaren Handlung bekannt, die den Wirkungsbereich der Dienststelle betrifft, der er angehört, so ist dies unverzüglich dem Leiter der Dienststelle zu melden.

Gemäß HinweisgeberInnenschutzgesetz können sich außerdem Hinweisgeber, insbesondere Mitarbeiter:innen 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 eingegangener Meldungen wird über einen Single-Point-of-Contact im Ressort sichergestellt.

Wien, 10. Oktober 2025

Eva-Maria Holzleitner, BSc

Unterzeichner	Bundesministerium für Frauen, Wissenschaft und Forschung
Datum/Zeit	2025-10-10T09:09:12+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.	641649373
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: http://www.bmfwf.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T09:15:29+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	