2667/AB
vom 10.10.2025 zu 3134/J (XXVIII. GP)

Bundesministerium
Europäische und internationale
Angelegenheiten

bmeia.gv.at

Mag.ª Beate Meinl-Reisinger, MES
Bundesministerin
Minoritenplatz 8, 1010 Wien,
Österreich

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Wien, am 10. Oktober 2025

GZ. BMEIA-2025-0.658.968

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen haben am 12. August 2025 unter der Zl. 3134/J-NR/2025 an mich eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Außenministerium sowie bei im Ausland tätigen Mitarbeiter:innen und Diplomaten“ gerichtet.

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

Zu den Fragen 1 bis 5 und 9 bis 11:

- *Welche verbindlichen Richtlinien bestehen derzeit im Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter:innen und Diplomaten?*
- *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 Dienststellen?*
  Wie oft finden diese Audits im Durchschnitt pro Jahr statt?
  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?*
  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 diplomatisches Personal 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?*
  Wenn ja, welche?
- *Inwieweit arbeitet das BMEIA mit nationalen und internationalen Stellen (z. B. DSN, CERT, EU Partner) zusammen, um sich über aktuelle Bedrohungen und Best Practices auszutauschen?*

Für das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten hohe Priorität. Für die Nutzung dienstlicher IT-Geräte sind die für die Bundesdienststellen geltenden Rechtsvorschriften anwendbar, insbesondere die Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV, BGBl. II Nr. 281/2009). Weiters gibt es interne Dienstanweisungen und Richtlinien, z.B. Richtlinien für den Einsatz von Mobilgeräten, Richtlinien am EDV-Arbeitsplatz, sowie Dienstanweisungen zur Informationssicherheit und Klassifizierung von BMEIA-internen Schriftstücken ebenso wie eine Dienstanweisung zu Aktentechnischer Sicherheit.

2025 wurde das Sicherheitskonzept für Mobilgeräte von einem externen Dienstleister neu überarbeitet. Es findet ein laufendes Monitoring der Dienstgeräte statt. Für Dienstreisen werden gemäß Länderbewertungen des BMEIA und des Bundesministeriums für Inneres (BMI) und der Direktion Staatsschutz und Nachrichtendienst (DSN) individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und „Good Practices“, wie z.B. den Handlungsempfehlungen der DSN, gesetzt. Im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zusätzlich führt das BMEIA 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 BMEIA zur Verfügung. Darüber

hinaus findet ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt. Das BMEIA arbeitet auch eng mit einschlägigen Diensten zusammen, insbesondere der DSN und dem *Government Computer Emergency Response Team* (CERT), und ist in die Zusammenarbeit im Wege der Koordinierungsstrukturen des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) eingebunden.

Für eine weitere Steigerung des Schutzniveaus wird derzeit das Rahmenwerk für ein Informationssicherheits- und Datenschutzmanagementsystem (ISMS/DSMS) im BMEIA erarbeitet, das sich an internationalen Sicherheitsstandards orientiert. Im Rahmen dieses Managementsystems wird sichergestellt, dass die jeweils geltenden Rechtsvorschriften und internen Regeln 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 werden. Dabei wird auch wie bisher die Expertise externer Stellen genutzt.

Die Untersuchung des eingangs erwähnten Sicherheitsvorfalls auch durch externe Experten lieferten keine Hinweise auf eine Sicherheitslücke im Verantwortungsbereich des BMEIA. Das BMEIA verfügt über umfassende Sicherungssysteme, die dienstliche Geräte bestmöglich vor einem unbefugten Zugriff schützen. Ein Abfließen von Kommunikationsdaten durch technisches Ausspähen konnte im genannten Fall nicht festgestellt werden. Darüber hinaus verweise ich auf die Beantwortung der parlamentarischen Anfrage ZI. 3122/J-NR/2025 vom 8. August 2025.

Zu Frage 6:

- *Wie werden die Mitarbeiter:innen des BMEIA 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 (z.B. Botschafter:innen, technische Attaches?) durchgeführt?

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

Zu Frage 7:

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

Das BMEIA verfügt über separate Teams für strategische und operative Angelegenheiten der Informationssicherheit und Cyberabwehr. Deren Zusammenarbeit wird durch das ISMS/DSMS in einem spezifischen Organisationsmodell geregelt. Da die Mitarbeiter im Bereich der Informationssicherheit in einem sensiblen Bereich tätig sind, wird aus Gründen der Informationssicherheit und des Datenschutzes von einer Nennung weiterer Details Abstand genommen.

Zu Frage 8:

- *Wie hoch war das jährliche Budget des BMEIA 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. Die Kosten für die derzeitig in Umsetzung befindliche Errichtung eines ISMS (Informationssicherheitsmanagementsystem), welches zu einer Erhöhung der Sicherheitsstandards beiträgt, betrugen im Jahr 2024 190.380 Euro und belaufen sich im aktuellen Budgetjahr bis August auf 269.875 Euro. Von einer detaillierten Auflistung der Maßnahmen und entsprechender Kosten zur Erhöhung bzw. dem Erhalt eines hohen IKT-Sicherheitsniveaus muss in Hinblick auf die Sicherung der Effektivität dieser Maßnahmen Abstand genommen werden.

Zu 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?

Es gibt etablierte Meldewege und -plattformen. Eine unverzügliche Behandlung wird durch das entsprechende interne Personal sichergestellt. Den Bediensteten des Ressorts stehen neben Führungskräften 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 der Bundesbediensteten oder 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 sie oder er angehört, so ist dies unverzüglich der Dienststellenleitung zu melden.

Gemäß HinweisgeberInnenschutzgesetz können sich außerdem Personen, einschließlich Mitarbeiterinnen und Mitarbeiter des Ressorts, bei Hinweisen auf 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“, dem Generalinspektorat, im Ressort sichergestellt.

Es darf auf die diesbezügliche Information zum HinweisgeberInnenschutzgesetz auf der Homepage des BKA verwiesen werden, unter https://www.bundeskanzleramt.gv.at/themen/compliance/hinweisgeberinnenschutzgesetz.html.

Mag.ª Beate Meinl-Reisinger, MES

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2025-10-10T16:53:38+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.	2062159656
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.bmeia.gv.at/verifizierung	

Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T16:55:48+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	