2653/AB
vom 10.10.2025 zu 3125/J (XXVIII. GP)

Bundesministerium Finanzen

bmf.gv.at

Dr. Markus Marterbauer
Bundesminister für Finanzen

Johannesgasse 5, 1010 Wien

Herrn Präsidenten
des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.646.364

Wien, 10. Oktober 2025

Sehr geehrter Herr Präsident!

Auf die schriftliche parlamentarische Anfrage Nr. 3125/J vom 12. August 2025 der Abgeordneten Süleyman Zorba, Kolleginnen und Kollegen beehre ich mich Folgendes mitzuteilen:

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 Regelungen hingewiesen werden:

- IKT-Nutzungsverordnung (IKT-NV), BGBl. II Nr. 281/2009
- Erlass des BMF „Informationssicherheit und Datenschutz im Arbeitsalltag“
- Erlass des BMF „Informationssicherheit und Datenschutz bei der IT-Beschaffung, der IT-Entwicklung und beim IT-Betrieb“
- Erlass des BMF „Nutzungsbedingungen für dienstliche Smartphones und Tablets“

Das Bundesministerium für Finanzen (BMF) 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 BMF zur Verfügung. Darüber hinaus findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt.

Zu Fragen 2 bis 5 und 9 bis 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 BMF hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das BMF verfügt daher über ein kombiniertes Informationssicherheits- und Datenschutz-Managementsystem, welches regelmäßig nach den internationalen Sicherheitsstandards ISO/IEC 27001 und ISO/IEC 27701 überprüft wird.

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 zum Beispiel 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 Evaluierung und Aktualisierung der diesbezüglichen Erlässe erfolgt laufend.

Die öffentlich verfügbaren Sicherheitsstandards ISO/IEC 27001 (Informationssicherheits-Management) und ISO/IEC 27701 (Datenschutz-Management) spezifizieren dafür umfassende Anforderungs- beziehungsweise Maßnahmenkataloge. Gemäß den Länderbewertungen des BMEIA und des BMI/DSN werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie zum Beispiel den Handlungsempfehlungen der Direktion Staatsschutz und Nachrichtendienst, 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?

Ja, es werden in regelmäßigen Abständen verpflichtende Schulungen angeboten und abgehalten. Die Schulungen werden auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Im Rahmen der Bildungsprogramme der Bundesfinanzakademie und 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?

Für das Management der Informationssicherheit – darunter fallen auch die IT-Sicherheit und die Cybersicherheit – ist die Stabsstelle Informationssicherheit der Präsidialabteilung 6 zuständig. Es darf in diesem Zusammenhang auf die Geschäfts- und Personaleinteilung des BMF verwiesen werden. Da die Mitarbeiterinnen und Mitarbeiter 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

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?

Ja, es gibt etablierte Meldewege und Plattformen. Eine unverzügliche Behandlung wird durch das entsprechende interne Personal sowie über zugekaufte Sicherheitsdienstleistungen sichergestellt.

Den Mitarbeiterinnen und Mitarbeitern des Ressorts stehen zusätzlich ihre Führungskräfte, der Informationssicherheitsbeauftragte gemäß § 7 InfoSiG, der Datenschutzbeauftragte, die Personalabteilungen sowie die Rechtsabteilung beratend und unterstützend zur Seite.

Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 (für Vertragsbedienstete in Verbindung mit § 5 Abs. 1 Vertragsbedienstetengesetz 1948) hingewiesen. Wird demnach den Bundesbediensteten in Ausübung ihres Dienstes der begründete Verdacht einer von Amts wegen zu verfolgenden gerichtlich strafbaren

Handlung bekannt, die den Wirkungsbereich der Dienststelle betrifft, denen sie angehören, so ist dies unverzüglich den Leiterinnen und Leitern der Dienststellen zu melden.

Darüber hinaus darf auf die diesbezügliche Information zum HinweisgeberInnenschutzgesetz auf der Homepage des BMF unter www.bmf.gv.at/services/hinweisgeberInnenschutzgesetz verwiesen werden.

Der Bundesminister:
Dr. Markus Marterbauer

Elektronisch gefertigt

Bundesministerium Finanzen	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bmf.gv.at/verifizierung
	Datum/Zeit	2025-10-10T08:03:29+02:00
Unterzeichner	Bundesministerium für Finanzen	
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.	874736968	
Dokumentenhinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T08:07:25+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	