Bundesministerium
Wohnen, Kunst, Kultur,
Medien und Sport

bmwkms.gv.at

**Andreas Babler, MSc**
Vizekanzler
Bundesminister für Wohnen, Kunst, Kultur,
Medien und Sport

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.652.162

Wien, 9. Oktober 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba, Freundinnen und Freunde haben am 12. August 2025 unter der **Nr. 3132/J** an mich eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen 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;
- diverse konkrete Handlungsempfehlungen wie zum Beispiel für den *Virtual Managed Desktop* (VMD), Empfehlung der Verwendung von *Key Pass* (Passwortverwaltungstool) oder „Sicheres Drucken“;
- Interne Informationen und Vorgaben zur Informationssicherheit.

Das Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport (BMWKMS) 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 BMWKMS 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 das BMWKMS hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Es werden daher gemeinsam mit dem Bundesrechenzentrum (BRZ) kontinuierlich Anpassungen und Weiterentwicklungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen, um das BMWKMS vor Bedrohungen zu schützen. Die öffentlich

verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

Dieses Vorgehen 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 zB 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 der vom Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) und dem Bundesministerium für Inneres bzw. der Direktion Staatsschutz und Nachrichtendienst (BMI/DSN) aktuellen Länderbewertungen werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie zB 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. Die Schulung und Sensibilisierung der Mitarbeiter:innen erfolgt sowohl in Präsenz als auch online über unterschiedliche Kanäle, insbesondere über das Intranet sowie per E-Mail. 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?*

Im BMWKMS ist hierfür die Abteilung I/A/8 sowie I/A/8/b – Referat IT zuständig. Ich darf auf die online abrufbare Geschäftseinteilung verweisen (https://www.bmwkms.gv.at/ministerium/geschaeftseinteilung.html).

**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 sichergestellt.

Den Mitarbeiter:innen des Ressorts stehen zusätzlich ihre Führungskräfte, die Informationssicherheitsbeauftragte gemäß § 7 InfoSiG, 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 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.

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

Andreas Babler, MSc

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WOHNEN, KUNST, KULTUR, MEDIEN UND SPORT @ AMTSSIGNATUR | Unterzeichner | Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport |
| | Datum/Zeit | 2025-10-10T11:25:38+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. | 479679199 |
| | Hinweis | Dieses Dokument wurde amtssigniert. |
| | Prüfinformation | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at |

| | | |
|---|---|---|
| | **Unterzeichner** | Parlamentsdirektion |
| | **Datum/Zeit-UTC** | 2025-10-10T11:31:30+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 | |