2655/AB
vom 10.10.2025 zu 3123/J (XXVIII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Christian Stocker
Bundeskanzler

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.645.987

Wien, am 10. Oktober 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Zorba, Kolleginnen und Kollegen haben am 12. August 2025 unter der Nr. **3123/J** eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Bundeskanzleramt sowie bei Mitarbeiter:innen in Schlüsselpositionen“ an mich gerichtet.

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

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
- ISMS Richtlinien (Richtlinie Informationssicherheit für Bedienstete, Leitlinie Informationssicherheit im Bundeskanzleramt)
- Leitlinie IKT-Sicherheit

- diverse konkrete Handlungsempfehlungen wie zum Beispiel für die „Sicherheit von iPhones“ oder „Vertraulicher Druck“

Das Bundeskanzleramt 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 Kommunikationsmittel des Bundeskanzleramts zur Verfügung.

Zu den 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 Bundeskanzleramt hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das Bundeskanzleramt verfügt daher über ein kombiniertes Informationssicherheits- und Datenschutz-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 Evaluierung und Aktualisierung der diesbezüglichen Erlässe erfolgt laufend. Die öffentlich verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

Gemäß den Länderbewertungen des Bundesministeriums für europäische und internationale Angelegenheiten und des Bundesministeriums für Inneres werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie z.B. 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:

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 verpflichtende Schulungen 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?*

Ich verweise hierzu auf die online abrufbare tagesaktuelle Geschäftseinteilung des Bundeskanzleramtes.

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?*

Grundsätzlich darf auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979 (für Vertragsbedienstete iVm § 5 Abs. 1 Vertragsbedienstetengesetz 1948) hingewiesen werden. Den Mitarbeiterinnen und Mitarbeitern des Ressorts stehen zusätzlich ihre Führungskräfte, der Informationssicherheitsbeauftragte gemäß § 7 InfoSiG, die Datenschutzbeauftragte, die Personalabteilung sowie die Rechtsabteilung beratend und unterstützend zur Seite.

Gemäß HinweisgeberInnenschutzgesetz können sich außerdem Hinweisgeberinnen und Hinweisgeber, insbesondere Mitarbeiterinnen und 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 Bundeskanzleramts unter https://www.bundeskanzleramt.gv.at/themen/compliance/hinweisgeberinnenschutzgesetz.html verwiesen werden.

Dr. Christian Stocker

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2025-10-10T08:39:26+02:00
	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.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T09:13:23+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	