Bundesministerium
Land- und Forstwirtschaft,
Klima- und Umweltschutz,
Regionen und Wasserwirtschaft

bmluk.gv.at

Mag. Norbert Totschnig, MSc
Bundesminister für Land- und Forstwirtschaft,
Klima- und Umweltschutz,
Regionen und Wasserwirtschaft

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.646.358

Ihr Zeichen: 3133/J-NR/2025

Wien, 10. Oktober 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleymann Zorba, Kolleginnen und Kollegen haben am 12. August 2025 unter der Nr. **3133/J** an mich eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz sowie bei Mitarbeiter:innen in Schlüsselpositionen“ gerichtet.

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

Zur Frage 1:

- Welche verbindlichen Richtlinien bestehen derzeit in Ihrem Haus zur sicheren Nutzung dienstlicher IT Geräte (Smartphones, Laptops, Tablets) durch Mitarbeiter:innen?

Das Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK) betreibt ein Informationssicherheits-Managementsystem (ISMS) nach anerkannten Best-Practice-Standards und stellt in diesem Rahmen verbindliche Richtlinien und Guidelines für die sichere Nutzung der genannten Geräte bereit.

Im Wesentlichen darf auf folgende Richtlinien hingewiesen werden:

- IKT-Nutzungsverordnung, BGBl. II Nr. 281/2009 idgF
- Datensicherheitsvorschrift des BMLUK
- Benutzer:innenrichtlinie für IT-Arbeitsplätze im BMLUK
- diverse konkrete Handlungsempfehlungen („Sicherheitspolicy von iDevices im BMLUK“, „Social Media Guidelines“ etc.).

Das BMLUK führt darüber hinaus Lage- und Risikobeurteilungen für Gefahren aus dem Cyber- und Informationsraum durch. Bei Bedarf werden aktuelle und konkrete Anleitungen sowie Empfehlungen hinsichtlich der internen Kommunikationsmittel des BMLUK zur Verfügung gestellt. Zudem findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Bundesministerien und den 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 BMLUK hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Neben dem unter der Frage 1 erwähnten ISMS betreibt das BMLUK auch eine eigene Plattform für den Schutz personenbezogener Daten zur Einhaltung der Datenschutz-Grundverordnung.

Diese Vorkehrungen sorgen unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken bestmöglich identifiziert, beurteilt und mittels geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden. Sie sehen 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 die Expertise externer Stellen genutzt, wie etwa von Computer-Notfallteams im Sinne des vierten Abschnitts des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018, und von qualifizierten Stellen im Sinne des § 3 Z 11 NISG.

Die Evaluierung und die Aktualisierung der diesbezüglichen Erlässe erfolgen laufend. Die öffentlich verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

Gemäß Länderbewertungen des Bundesministeriums für europäische und internationale Angelegenheiten sowie des Bundesministeriums für Inneres bzw. der Direktion Staatsschutz und Nachrichtendienst (DSN) werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good-Practices, wie beispielsweise den Handlungsempfehlungen der DSN, gesetzt.

Im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zur 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?

Im BMLUK werden für Mitarbeiterinnen und Mitarbeiter zyklisch Awareness-Schulungen durchgeführt, aber auch sonstige Bewusstseinsbildungsmaßnahmen (wie z. B. Online-Awareness-Trainings, gezielte Informationskampagnen, Erlass von Richtlinien) gesetzt. Darüber hinaus werden aktuelle Informationen anlassbezogen über das Intranet des BMLUK zum Thema Cybersicherheit bereitgestellt. Im Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich genutzt.

Zur 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?

Die Aufgabenwahrnehmung zur Bekämpfung der Cyberkriminalität obliegt dem Bundesministerium für Inneres. Innerhalb des BMLUK werden diese Agenden vom Chief-Information-Security-Officer (CISO) des BMLUK in enger Zusammenarbeit und Abstimmung mit dem Abteilungsleiter der IKT-Abteilung und Chief-Information-Officer sowie dem Chief-Digital-Officer des Ressorts strategisch wahrgenommen und mit Fachexpertinnen und -experten koordiniert.

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.

Zur 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.

Zur 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?

Das BMLUK betreibt einen eigenen IKT-Help-Desk, der den Mitarbeiterinnen und Mitarbeitern zu den Bürozeiten persönlich zur Verfügung steht. Darüber hinaus können ungewöhnliche Vorfälle auch auf elektronischem Weg an diese Stelle gemeldet werden. Die Behandlung der Meldungen wird durch ein eigenes Notfallmanagement für IT-Notfälle sichergestellt.

Den Mitarbeiterinnen und Mitarbeitern des BMLUK stehen zusätzlich die Führungskräfte, der CISO, die Informationssicherheitsbeauftragte gemäß § 7 Informationssicherheitsgesetz, BGBl. I Nr. 23/2002 idgF, der Datenschutzbeauftragte und die Personalabteilung beratend und unterstützend zur Seite.

Darüber hinaus wird auf die Meldepflicht gemäß § 53 Abs. 1 Beamten-Dienstrechtsgesetz 1979, BGBl. Nr. 333/1979 idgF, bzw. § 5 Abs. 1 Vertragsbedienstetengesetz 1948, BGBl. Nr. 86/1948 idgF, hingewiesen. Wird demnach der bzw. 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 bzw. er angehört, so ist dies unverzüglich der Leitung der Dienststelle zu melden.

Gemäß HinweisgeberInnenschutzgesetz (HSchG), BGBl. I Nr. 6/2023 idgF, können sich außerdem Hinweisgeberinnen und -geber, insbesondere Mitarbeiterinnen und Mitarbeiter des BMLUK, bei Rechtsverletzungen – auf Wunsch auch anonym – an die zuständige interne Meldestelle (Bundesdisziplinarbehörde) bzw. an die zuständige externe Meldestelle für das BMLUK (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung) wenden.

Weitere Informationen zum HSchG werden im Intranet des BMLUK bereitgestellt.

Mag. Norbert Totschnig, MSc

Bundesministerium Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft	Unterzeichner	Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft
	Datum/Zeit	2025-10-10T09:46:20+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.	1197990292
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: https://www.bmluk.gv.at/amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T09:50:57+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	