2652/AB
vom 10.10.2025 zu 3127/J (XXVIII. GP)

Bundesministerium
Bildung

bmb.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.647.812

Die schriftliche parlamentarische Anfrage Nr. 3127/J-NR/2025 betreffend IT- und Cybersicherheit im Bildungsministerium sowie bei Mitarbeiter:innen in Schlüsselpositionen, die die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen am 12. August 2025 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

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

Folgende Richtlinien werden im Bundesministerium für Bildung angewendet:

- IKT-Nutzungsverordnung (IKT-NV), BGBl. II Nr. 281/2009 idgF.,
- Richtlinie zur Nutzung von Notebooks,
- Smartphone-Richtlinie,
- diverse konkrete Handlungsempfehlungen, wie zum Beispiel die Passwortrichtlinie für PCs bzw. Notebooks.

Das Bundesministerium für Bildung führt 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 Bundesministeriums für Bildung zur Verfügung. Darüber hinaus findet auch ein regulärer und anlassbezogener Informationsaustausch zwischen den Ministerien und obersten Organen statt.

Zu den Fragen 2 bis 5 sowie 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 Bundesministerium für Bildung hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das Bundesministerium für Bildung 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 werden. Dabei wird auch die Expertise externer Stellen genutzt, wie zB. von Computer-Notfallteams im Sinne des vierten Abschnitts des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018 idgF., 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 / Direktion Staatsschutz und Nachrichtendienst 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:

- *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 Schulungen angeboten und abgehalten. Die Schulungen werden auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Im Rahmen der Grundausbildung erfolgt eine grundlegende Schulung im Rahmen des Fachs Datenschutz und IT-Sicherheit. Weiters werden über das Bildungsprogramm der Verwaltungsakademie des Bundes umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Themenbereich 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?

In der Geschäftseinteilung des Bundesministeriums für Bildung ist Abteilung Präs/13 – „IT-Services Zentralstelle“ dafür vorgesehen.

Da die 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 schon deswegen nicht eindeutig zuordenbar.

Für Ausgaben in Belangen der IT- und Cybersicherheit sind entsprechend der Kontenplanverordnung 2013 idgF. in der Untergliederung 30 (Bildung) keine eigenen (Verrechnungs-)Konten vorgesehen. Die Ausgaben sind sachlich zugeordnet bei einschlägigen Detailbudgets und Konten für ADV-Aufwand – etwa beim Konto 7278.090 (Werkleistungen ADV) der Detailbudgets 30.01.01 und 30.01.04 – mitveranschlagt und in den in den jährlichen Bundesvoranschlägen dort ausgewiesenen Gesamtbeträgen enthalten. Aus diesem Grunde sind auch dahingehende Auswertungen aus dem Haushaltsverrechnungssystem des Bundes nicht möglich.

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 Mitarbeitern des Ressorts stehen zusätzlich ihre Führungskräfte, der Informationssicherheitsbeauftragte gemäß § 7 InfoSiG, die Datenschutzbeauftragten, die Personalabteilung sowie die Interne Revision 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 Meldestelle wenden. Eine rasche Bearbeitung eingegangener Meldungen wird über einen Single-Point-of-Contact im Ressort sichergestellt.

Wien, 10. Oktober 2025

Christoph Wiederkehr, MA

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung
	Datum/Zeit	2025-10-10T07:21:48+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.	2097799830
	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.bmb.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T07:31:41+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	