Bundesministerium
Justiz

bmj.gv.at

Dr.in Anna Sporrer
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.647.688

Ihr Zeichen: BKA - PDion (PDion)3130/J-NR/2025

Wien, am 10. Oktober 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen haben am 12. August 2025 unter der Nr. **3130/J-NR/2025** an mich eine schriftliche parlamentarische Anfrage betreffend „IT- und Cybersicherheit im Justizministerium 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?*

Als maßgebliche verbindliche Richtlinie für die Nutzung dienstlicher IT-Geräte (Smartphones, Laptops, Tablets) gilt für Mitarbeiter:innen des Bundesministeriums für Justiz neben der IKT-Nutzungsverordnung (IKT-NV), BGBl. II Nr. 281/2009 die IKT-Benutzungsrichtlinie in jeweils letztgültiger Fassung.

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 Bundesministerium für Justiz hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Anwendungen und IKT-Infrastrukturkomponenten eine hohe Priorität. Das Bundesministerium für Justiz verfügt daher über ein Informationssicherheits-Managementsystem, welches sich an internationalen Standards 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 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.

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 (BMEIA) und der Direktion Staatsschutz und Nachrichtendienst im Bundesministerium für Inneres (BMI/DSN) werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie zB. die 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.

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 Rahmen des Bildungsprogramms der Verwaltungsakademie des Bundes werden umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Bereich angeboten (z.B. „Cybersicherheit“). Es werden in regelmäßigen Abständen verpflichtende Schulungen angeboten und abgehalten, welche auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst sind.

Seit 2022 haben alle in die Justiz Neueintretenden ein justizeigenes eLearning-Modul zum Thema „IT-Sicherheit“ verpflichtend zu absolvieren. Das Modul basiert auf der IKT-Benutzungsrichtlinie der Justiz und behandelt zusammengefasst folgende Bereiche: Verhalten bei IT-Problemen, Sicherheit am IT-Arbeitsplatz, Umgang mit Hard- und Software, Umgang mit Daten, Verhalten bei Datenverlust und Datenleck, Internet-Nutzung, E-Mail sowie Verwendung von Diensthandys etc. Die ordnungsgemäße Absolvierung wird in regelmäßigen Abständen überprüft.

Allen bereits zuvor eingetretenen Justizmitarbeiter:innen wird die Absolvierung des eLearning-Moduls nachdrücklich empfohlen. Insgesamt wurde das Modul von über 7.400 Justizbediensteten aller Berufsgruppen abgeschlossen.

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?*

Der Abteilung III 3 Rechtsinformatik, Informations- und Kommunikationstechnologie obliegt auch die Zuständigkeit für IT-Sicherheit und Cyberabwehr im BMJ.

Da die Mitarbeiter:innen 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 und keine gesonderte Budgetierung für die Beschaffungen iZm IT- und Cybersicherheit erfolgt, 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?*

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

Den Mitarbeiter:innen des Bundesministeriums für Justiz stehen zusätzlich ihre Führungskräfte, der 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:innen, insbesondere Mitarbeiter des Bundesministeriums für Justiz, 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 Bundesministerium für Justiz sichergestellt. Mit 10. Juli 2023 wurde die webbasierte interne Meldestelle des Justizressorts aktiv geschaltet (abrufbar sowohl im Intranet als auch im Internet).

Diese Hinweisgeber:innen-Plattform steht Bediensteten der Justiz zur Verfügung, die Informationen über allfällige im Raum stehende Verstöße gegen die Compliance Leitlinien der Justiz oder über Rechtsverletzungen nach dem HinweisgeberInnenschutzgesetz (HSchG) erlangt haben. Ferner können über diese Plattform auch Hinweise und Meldungen zu Diskriminierung, (sexueller) Belästigung oder Gewalt im Arbeitsumfeld der Justiz abgegeben werden.

Sofern eine Meldung bei der internen Meldestelle des Justizressorts einlangt, wird davon unmittelbar die Leitung der internen Meldestelle des Justizressorts verständigt.

Dr.[in] Anna Sporrer

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2025-10-10T11:35:30+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-10T11:37:41+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	