

 **Bundesministerium**  
Inneres

**Karl Nehammer, MSc**  
Bundesminister

Herrn  
Präsidenten des Nationalrates  
Mag. Wolfgang Sobotka  
Parlament  
1017 Wien

Geschäftszahl: 2021-0.740.557

Wien, am 22. November 2021

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Jan Krainer, Genossinnen und Genossen haben am 22. September 2021 unter der Nr. **7928/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Informationssicherheitssysteme“ gerichtet.

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

**Zu den Fragen 1 bis 5:**

- *Welche Vorschriften bilden den Rahmen für die sichere Behandlung von Informationen im Wirkungsbereich Ihres Ressorts?*
- *Findet die Geheimschutzordnung des Bundes in Ihrem Ressort Anwendung?*
- *Findet das Informationssicherheitsgesetz in Ihrem Ressort Anwendung?*
- *Findet die Verschlusssachenverordnung der Bundesregierung in Ihrem Ressort noch Anwendung?*
- *Haben Sie für Ihr Ressort eigenständige Vorschriften erlassen und wenn ja, welche?*

Der Rahmen für die sichere Behandlung von Informationen bilden das Informationssicherheitsgesetz (InfoSiG), die Informationssicherheitsverordnung (InfoSiV), die Geheimschutzordnung des Bundes (GehSo), die Richtlinie des Bundesministeriums für Inneres zur Geheimschutzordnung des Bundes sowie interne Rundschreiben. Zur Konkretisierung der genannten Rechtsnormen wurden des weiteren Dienstanweisungen zur administrativen

Behandlung des nachrichtendienstlichen und sonstigen klassifizierten Posteingangs erlassen.

Die Verschlusssachenverordnung ist eine Verordnung des Bundesministeriums für Justiz, deren Geltungsbereich gemäß ihres § 1 Abs. 2 für die Zentralstelle des Bundesministeriums für Justiz und alle weiteren Dienststellen im Bereich des Justizressorts sowie die ordentlichen Gerichte festgelegt ist. Die Verschlusssachenverordnung fällt daher nicht in meinen Vollzugsbereich.

**Zur Frage 6:**

- *Findet die ÖNORM S 2450 in Ihrem Ressort Anwendung?*

Nein, da die ÖNORM S2450 allgemeine Sicherheitsanforderungen für industrielle und andere Unternehmen festlegt, die im Rahmen von Auftragsverfahren Zugang zu klassifizierten Informationen erlangen wollen. Damit definiert sie die Rahmenbedingungen für die Erlangung einer Sicherheitsunbedenklichkeitsbescheinigung gemäß Informationssicherheitsgesetz.

Das Bundesministerium für Inneres ist daher nicht Adressat der ÖNORM S2450.

**Zu den Fragen 7 und 8:**

- *Besteht in Ihrem Ressort ein Informationssicherheitssystem einschließlich eines Prozesses zur Schulung, Umsetzung und Kontrolle von Informationssicherheitsvorschriften?*
- *Wurde dieses System nach ÖNORM S 2450 überprüft?*

Ja. Dieses Informationssicherheitssystem wurde nicht nach der für das Bundesministerium für Inneres nicht anwendbaren ÖNORM S2450 überprüft, sondern von der Informationssicherheitskommission (ISK) akkreditiert.

Gemäß § 8 Informationssicherheitsgesetz wurde eine Informationssicherheitskommission eingerichtet, der die Informationssicherheitsbeauftragten aller Bundesministerien angehören. Den Vorsitz führt der Informationssicherheitsbeauftragte des Bundeskanzleramtes. Die Informationssicherheitskommission hat

- auf eine bundesweite Einheitlichkeit von Schutzmaßnahmen und deren Koordination im Bereich der Bundesverwaltung, insbesondere bei der Leistung von Amtshilfe nach § 5 leg.cit., hinzuwirken,

- einen Erfahrungsaustausch hinsichtlich der Einhaltung von Schutzmaßnahmen nach § 7 Abs. 2 leg.cit. im jeweiligen Ressortbereich durchzuführen und gegebenenfalls Vorschläge zur Verbesserung der Informationssicherheit zu erstatten,
- der Bundesregierung bei Bedarf, jedoch mindestens alle drei Jahre, einen Bericht über den Stand der Informationssicherheit auf Grundlage von Beiträgen der einzelnen Informationssicherheitsbeauftragten zu erstatten,
- Maßnahmen zum Schutz des Austausches klassifizierter Informationen zwischen Österreich und internationalen Organisationen, sonstigen zwischenstaatlichen Einrichtungen oder fremden Staaten zu setzen beziehungsweise vorzuschlagen, sofern sie zur Durchführung der mit diesen über den Schutz und die Sicherheit klassifizierter Informationen getroffenen Vereinbarungen erforderlich sind,
- Sicherheitsunbedenklichkeitsbescheinigungen für Personen, Unternehmen, Einrichtungen und Anlagen auszustellen.

In ihrer Eigenschaft als National Security Authority ist die Informationssicherheitskommission für die sichere Verwendung klassifizierter Informationen in den Bereichen personelle Sicherheit, physische Sicherheit, Dokumentensicherheit/Registerführung sowie im Bereich der Verarbeitung klassifizierter Informationen mittels IKT (Information Assurance) zuständig und übt die Aufgabenstellung einer nationalen Akkreditierungsbehörde ("SAA - Security Accreditation Authority") für innerstaatliche Einrichtungen im zivilen Bereich aus.

#### **Zu den Fragen 9 und 10:**

- *Besteht in Ihrem Ressort eine zentrale Koordinationsstelle für Fragen der Informationssicherheit?*
- *Welche Aufgaben sind dieser Koordinationsstelle zugeteilt?*

Ja, als zentrale Koordinationsstelle fungiert der Informationssicherheitsbeauftragte, dessen Aufgaben dem § 4 Abs. 2 Informationssicherheitsverordnung zu entnehmen sind.

#### **Zu den Fragen 11 bis 15:**

- *Welche Arten bzw. Stufen der Geheimhaltung sehen diese Vorschriften für welche Arten von Dokumenten vor?*
- *Nach welchen Kriterien erfolgt die Zuordnung von Akten und Unterlagen zu bestimmten Schutzstufen?*

- *Welche organisatorischen Maßnahmen werden je nach Stufe zum Schutz sensibler Informationen getroffen?*
- *Welche physischen Maßnahmen werden je nach Stufe zum Schutz sensibler Informationen getroffen?*
- *Welche persönlichen Maßnahmen werden je nach Stufe zum Schutz sensibler Informationen getroffen?*

Die Arten bzw. Stufen der Geheimhaltung sind § 2 Informationssicherheitsgesetz bzw. § 3 Geheimschutzordnung des Bundes zu entnehmen.

Die je nach Stufe der Geheimhaltung zu treffenden organisatorischen, physischen und persönlichen Maßnahmen zum Schutz der klassifizierten Information ergeben sich auf Grund der gesetzlichen Vorgaben.

**Zur Frage 16:**

- *Wann fand die letzte Überprüfung des Informationssicherheitssystems in Ihrem Ressort statt?*

Der Akkreditierungsprozess des Büros der Informationssicherheitskommission wird mit einem „approval to operate“ abgeschlossen, dieses wird befristet erteilt und ist nach Ablauf zu erneuern. Exakte Daten und Zeitabläufe können auf Grund der Verpflichtung zur Wahrung der Amtsverschwiegenheit nicht bekannt gegeben werden.

**Zur Frage 17:**

- *Welche Maßnahmen wurden im Zuge dieser Überprüfung empfohlen?*

Informationen zu Maßnahmen können im Hinblick auf die IT-Sicherheit des Systems und auf Grund des Interesses der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit nicht im Zuge einer öffentlichen Beantwortung einer parlamentarischen Anfrage bekannt gegeben werden.

**Zu den Fragen 18 bis 25:**

- *Wie viele Akten und Unterlagen der Stufe "Eingeschränkt" (oder vergleichbar) bestehen in der Zentralstelle Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*

- d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Eingeschränkt“ (oder vergleichbar) bestehen in nachgelagerten Dienststellen Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*
  - d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Vertraulich“ (oder vergleichbar) bestehen in der Zentralstelle Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*
  - d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Vertraulich“ (oder vergleichbar) bestehen in nachgelagerten Dienststellen Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*
  - d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Geheim“ (oder vergleichbar) bestehen in der Zentralstelle Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*
  - d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Geheim“ (oder vergleichbar) bestehen in nachgelagerten Dienststellen Ihres Ressorts?*
  - a. Wie viele davon sind nationalen Ursprungs?*
  - b. Wie viele davon sind EU-Ursprungs?*
  - c. Wie viele davon sind NATO-Ursprungs?*
  - d. Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*

- *Wie viele Akten und Unterlagen der Stufe „Streng Geheim“ (oder vergleichbar) bestehen in der Zentralstelle Ihres Ressorts?*
  - a. *Wie viele davon sind nationalen Ursprungs?*
  - b. *Wie viele davon sind EU-Ursprungs?*
  - c. *Wie viele davon sind NATO-Ursprungs?*
  - d. *Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*
- *Wie viele Akten und Unterlagen der Stufe „Streng Geheim“ (oder vergleichbar) bestehen in nachgelagerten Dienststellen Ihres Ressorts?*
  - a. *Wie viele davon sind nationalen Ursprungs?*
  - b. *Wie viele davon sind EU-Ursprungs?*
  - c. *Wie viele davon sind NATO-Ursprungs?*
  - d. *Wie viele davon sind anderen Ursprungs und jeweils welcher Organisation zuordenbar?*

Zur Protokollierung von Informationen der Stufe EINGESCHRÄNKT (oder vergleichbar) besteht keine rechtliche Vorgabe, weshalb diese Fragen keiner Beantwortung zugänglich sind. Informationen über die Anzahl von Akten oder Unterlagen, die im Bundesministerium für Inneres als „vertraulich“ oder höher eingestuft sind, sind als EINGESCHRÄNKT oder höher klassifiziert und unterliegen der Amtsverschwiegenheit.

Die Anzahl der Dokumente, die auf Grund völkerrechtlicher Verpflichtungen geschützt werden, kann darüber hinaus auf Grund des diesbezüglichen Vertrauensverhältnisses nicht der Öffentlichkeit zugänglich gemacht werden.

**Zu den Fragen 26 bis 34 und 36:**

- *Wie viele Personen in der Zentralstelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Eingeschränkt“ berechtigt?*
- *Wie viele Personen in der Zentralstelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Vertraulich“ berechtigt?*
- *Wie viele Personen in der Zentralstelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Geheim“ berechtigt?*
- *Wie viele Personen in der Zentralstelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Streng geheim“ berechtigt?*
- *Wie viele Personen in nachgelagerten Dienststelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Eingeschränkt“ berechtigt?*
- *Wie viele Personen in nachgelagerten Dienststelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Vertraulich“ berechtigt?*

- *Wie viele Personen in nachgelagerten Dienststelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Geheim“ berechtigt?*
- *Wie viele Personen in nachgelagerten Dienststelle Ihres Ressorts sind zum Zugriff auf Informationen der Stufe „Streng Geheim“ berechtigt?*
- *Wie vielen externen Personen wurde der Zugriff auf besonders geschützte Informationen der verschiedenen Schutzstufen Ihres Ressorts gewährt und aus welchem jeweiligen Grund?*
- *Wie viele Personen Ihres Kabinetts sind berechtigt, auf Informationen welcher Schutzstufe zuzugreifen?*

Die Zugangsvoraussetzungen ergeben sich aus den maßgeblichen gesetzlichen Bestimmungen. Bedienstete erhalten nur Zugang zu jenen Informationen, welche für die Erfüllung ihrer dienstlichen Aufgaben erforderlich sind ("Need to know"-Prinzip). Informationen über den Zugang zu klassifizierten Informationen können auf Grund der Verpflichtung zur Wahrung der Amtsverschwiegenheit nicht veröffentlicht werden.

**Zur Frage 35:**

- *Welche technischen Vorkehrungen werden je nach Stufe für den Schutz sensibler Informationen, die elektronisch verarbeitet werden, getroffen?*

Die Voraussetzungen zur elektronischen Verarbeitung von klassifizierten Informationen ergeben sich aus der Informationssicherheitsverordnung und den Richtlinien und Vorgaben der Informationssicherheitskommission. Konkrete technische Vorkehrungen, die Angriffsvektoren in der Zukunft bilden könnten, unterliegen der Amtsverschwiegenheit.

**Zur Frage 37:**

- *Wurden Sie selbst über den sicheren Umgang mit Informationen der jeweiligen Schutzstufe belehrt?*

Nach § 1 Abs. 2 Informationssicherheitsgesetz gelten die Voraussetzungen für den Zugang zu klassifizierten Informationen nach § 3 Abs. 1 nicht für den Bundespräsidenten, den Bereich des Nationalrates und des Bundesrates, die Mitglieder der Bundesregierung, die Staatssekretäre, die Gerichtsbarkeit, den Verfassungsgerichtshof und den Verwaltungsgerichtshof, den Rechnungshof und die Volksanwaltschaft. Die Weitergabe von klassifizierten Informationen an diese Organe und Einrichtungen unterliegt keinen Beschränkungen nach diesem Bundesgesetz, jedoch völkerrechtlich vorgesehenen Einschränkungen.

**Zu den Fragen 38 bis 43:**

- *Wie viele Personen in der Zentralstelle Ihres Ressorts haben Zugriff auf das Extranet des Rates?*
- *Wie viele Personen in nachgelagerten Dienststellen Ihres Ressorts haben Zugriff auf das Extranet des Rates?*
- *Wie viele externe Personen haben im Wirkungsbereich des Ressorts Zugriff auf das Extranet des Rates?*
- *Wie viele Personen in der Zentralstelle Ihres Ressorts haben Zugriff auf das Extranet-R des Rates der EU?*
- *Wie viele Personen in nachgelagerten Dienststellen Ihres Ressorts haben Zugriff auf das Extranet-R des Rates der EU?*
- *Wie viele externe Personen haben im Wirkungsbereich des Ressorts Zugriff auf das Extranet-R des Rates?*

Das Extranet des Rates ist ein System, das im April 2021 stillgelegt wurde. An dessen Stelle ist für allgemeine Rats-Informationen das Delegates Portal und für klassifizierte Informationen das Delegates Portal – R getreten. Der Zugang richtet sich nach dem Umfang der dienstlichen Aufgaben der Mitarbeiterinnen und Mitarbeiter meines Ressorts.

**Zur Frage 44:**

- *Wie viele Personen im Wirkungsbereich Ihres Ressorts haben Zugriff auf ein Tempest-Netzwerk und zu welchem Zweck?*

Auf Grund der Verpflichtung zur Wahrung der Amtsverschwiegenheit nehme ich davon Abstand, Informationen über den Zugang zu hochklassifizierten Systemen, die TEMPEST-geschützte Geräte beinhalten, zu erteilen.

Karl Nehammer, MSc





