Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Johannes Rauch
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2024-0.446.167

Wien, 25.7.2024

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 18864/J des Abgeordneten Christian Hafenecker, MA betreffend Wie steht es um die Datensicherheit des Bundes?** wie folgt:

Fragen 1 und 3:

- *Wie viele Cyberangriffe verzeichnete Ihr Ressort in der laufenden Legislaturperiode?*
    a. *Wie viele dieser Cyberangriffe waren erfolgreich, konnten also Schaden anrichten (Datendiebstahl, Lahmlegung, DDos etc.)?*
    b. *Sofern bekannt, aus welchen Ländern/Regionen stammten diese Cyberangriffe (bitte um Auflistung)?*
- *Wie viele Cyberangriffe verzeichneten nachgeordnete Dienststellen Ihres Ressorts in der laufenden Legislaturperiode?*
    a. *Welche nachgeordneten Dienststellen waren betroffen?*
    b. *Wie viele dieser Cyberangriffe waren erfolgreich, konnten also Schaden anrichten (Datendiebstahl, Lahmlegung, DDos etc.)?*
    c. *Sofern bekannt, aus welchen Ländern/Regionen stammten diese Cyberangriffe (bitte um Auflistung)?*

Es darf auf die Beantwortung der parlamentarischen Anfrage Nr. 18819/J („Mögliche Hackerangriffe auf Ihr Ministerium“) vom 12.06.2024 (XXVII. GP) verwiesen werden.

Frage 2: *Gibt es eine zentrale Stelle innerhalb Ihres Ressorts oder innerhalb der Bundesverwaltung, an die derartige Vorfälle gemeldet werden bzw. gemeldet werden müssen (Stichwort Lagebild)?*

a. Wer führt ein solches Lagebild?

Innerhalb des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) zeichnet die Abteilung I/B/8 Informationstechnologie und –management für die Erkennung und Behandlung von Cyberangriffen im Bereich Soziales verantwortlich.

Für den Bereich Gesundheit (Sektionen VI und VII) zeichnet die Abteilung VI/B/10 für die Erkennung und Behandlung von Cybersicherheitsvorfällen verantwortlich. Im Falle von Vorkommnissen erfolgt die Abstimmung mit der Abteilung I/B/8 Informationstechnologie und -management mit allen vorgesehenen Folgemaßnahmen.

Die Abteilung I/B/8 erstellt das ressortinterne Lagebild bei Cyber Security Vorfällen in Abstimmung mit dem ICT Service Provider und ggf. dem GovCERT. Diese Informationen fließen – abhängig vom konkreten Vorfall – in das durch den gemäß NISG eingerichteten IKDOK (Innerer Kreis der Operativen Koordinierung), welcher das gesamtstaatliche Lagebild erstellt.

Frage 4: *Mit welchen ausländischen IT-Konzernen arbeitet Ihr Ressort derzeit in welchen Bereichen zusammen (Bitte um Auflistung nach Name und Land)?*

a. Welche Verträge bestehen mit welchen ausländischen IT-Konzernen?
b. Welche konkreten Dienstleistungen werden in Anspruch genommen?
c. Zu welchen Dienstleistungen gab es Ausschreibungen?

Bei der Beschaffung von IKT Leistungen bedient sich das BMSGPK vorrangig des Bundesrechenzentrums (BRZ) und BBG gelisteter Produkte und Dienstleistungen. Nicht derartig beschaffbare Leistungen werden gemäß Bundesvergabegesetz und unter Einhaltung der entsprechenden gesetzlichen Rahmenbedingungen (wie z.B. DSGVO) beschafft.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Fragen 5 und 6:

- *Wo und wie werden digital generierte Daten (personenbezogene wie nichtpersonenbezogene) durch Ihr Ressort konkret gesichert?*
    a. *Sofern Cloud-Lösungen in Anspruch genommen werden, welche und in welchen Staaten liegen die dazugehörigen Server?*
    b. *Welche externen Dienstleister haben Zugriff auf welche Daten in Ihrem Ressort?*
- *Wo werden Daten-Backups Ihres Ressorts konkret gesichert?*
    a. *Sofern Cloud-Lösungen in Anspruch genommen werden, welche und in welchen Staaten liegen die dazugehörigen Server?*
    b. *Wer hat Zugriff auf diese Backups?*
    c. *Hat Ihr Ressort jederzeit Zugriff auf diese Backups?*
    d. *Haben externe Dienstleister oder Dritte Zugriff auf diese Backups (Bitte um Auflistung)?*

Das BMSGPK verfolgt bei der Verarbeitung von Daten einen risikobasierten Ansatz. Abhängig von der Schutzwürdigkeit der Daten, werden diese gegebenenfalls unter Einsatz starker Verschlüsselung und georedundant gespeichert. Je nach Kritikalität der Daten ist der Zugriff auf bestimmte Personengruppen eingeschränkt.

Frage 7: *Welche konkreten Maßnahmen und Sicherheitsstrategien verfolgt Ihr Ressort, um möglichen Missbrauch mit Daten durch Dritte zu verhindern?*

Daten werden im BMSGPK im risikobasierten Ansatz geschützt, darüber hinaus wird ein gesamtheitlicher Ansatz verfolgt, welcher Maßnahmen nach dem „Stand der Technik“ sowie organisatorisch entsprechend umsetzt.

Frage 8: *Gibt es zwischen den ressortübergreifenden Abstimmungen, gemeinsame Arbeitsgruppen, Organisationseinheiten oder ähnliches im Bereich IT-Sicherheit und Cybersecurity hinsichtlich Synergien, Wissen, Effizienz, Lagebewusstsein, Gefährdungspotenzial und ähnlichem?*

Im Bereich der IT-Sicherheit und Cybersecurity gibt es sowohl auf strategischer, operativer als auch technischer Ebene interministerielle Arbeits- und Austauschgruppen. Als Beispiel seien hier genannt die Cyber Sicherheit Steuerungsgruppe (CSS), der Austrian Trust Circle Government (ATC-Gov) und die Cyber Sicherheit Plattform (CSP).

Das durch den Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) erstellte Cyberlagebild wird dem BMSGPK zur Verfügung gestellt.

Hinsichtlich der speziellen, heterogenen IT-Technologien und -Infrastrukturen im Gesundheitsbereich sind insbesondere auf Basis der Artikel 15a B-VG Vereinbarung über die Organisation und Finanzierung des Gesundheitswesens spezielle Cybersicherheitsstrukturen etabliert, die in enger Abstimmung mit jenen des Bundes agieren. Im Gesundheitssektor finden – mit Schwerpunkt auf Systeme in Krankenanstalten – vernetzte Systeme im Bereich der Medizinprodukte, Blut- und Gewebesicherheit u.dgl. regelmäßige Übungen auch auf EU-Ebene statt.

Fragen 9 und 10:

- *Wie ist der Stand der NIS-Richtlinien-Umsetzung in Ihrem Ministerium?*
- *Wurden die aktuellen Umsetzungen der NIS-Richtlinien evaluiert?*
    a. *Wenn ja, mit welchen Ergebnissen?*
    b. *Wenn nein, warum nicht bzw. ist eine Evaluierung geplant? Wann?*

Das Netz- und Informationssystemsicherheitsgesetz (NISG) legt Maßnahmen fest, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung erreicht werden soll. Das BMSGPK hat die gemäß § 22 geforderten Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen der öffentlichen Verwaltung im Rahmen des Security Framework Bund (SFB) bewertet und durch das NIS-Audit dokumentiert.

Die Bewertung der Eignung der Sicherheitsmaßnahmen erfolgt auf kontinuierlicher Basis unter Abstützung auf den Risikoeinschätzungen und technischen Empfehlungen des IKDOK.

Fragen 11, 12 und 13:

- *Gibt es Anstrengungen, Vorhaben oder Überlegungen, die Datenverarbeitung seitens der Bundesverwaltung in Österreich zu bewerkstelligen?*
- *Welche Datenarchive im Wirkungsbereich des Bundes liegen im Ausland (Bitte um Auflistung)?*
- *Welche Anstrengungen unternimmt die Bundesregierung, um sämtliche Datenarchive auf österreichisches Staatsgebiet zu holen und somit gerade in Krisenzeiten ein Mindestmaß an digitaler Autonomie und Sicherheit zu gewährleisten?*

Die Datenverarbeitung erfolgt im BMSGPK nach Analyse hinsichtlich der Klassifizierung, Kritikalität, Verfügbarkeitsanforderungen und Datenschutzanforderungen abgestuft lokal, auf ministerieller Infrastruktur, auf Bundesinfrastruktur oder auf Infrastruktur von Drittanbietern. Wo eine Datenverarbeitung durch Dritte wahrgenommen wird, erfolgt dies nach erfolgter Risikobewertung und unterliegt den strengen Regelungen der DSGVO.

Mit der Bundesrechenzentrum GmbH wurde ein gesetzlicher Dienstleister eingerichtet, welcher im 100%igem Eigentum des Bundes steht. Als solcher ist er zentraler IT Dienstleister des Bundes und auf österreichischem Staatsgebiet tätig.

Darüber hinaus gibt es unterschiedliche Projekte um die Abhängigkeit von Dritten zu reduzieren.

Frage 14: *Welche Position nimmt die Bundesregierung zum US-„Cloud Act'' in Hinblick auf die DSGVO ein?*

Die Einhaltung der Vorschriften der DSGVO durch Verantwortliche, die gemäß Art. 2 und 3 DSGVO der DSGVO unterliegen, obliegt dem für die jeweilige Datenverarbeitung Verantwortlichen (vgl. Art. 24 DSGVO). Dies gilt auch im Falle eines Drittlandbezugs (etwa im Zusammenhang mit der Nutzung von Clouds).

Im Hinblick auf Datenübermittlungen an Drittländer ist auf die Vorschriften von Kapitel V DSGVO hinzuweisen, insbesondere auf Art. 48 DSGVO, demzufolge „[j]egliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, […] unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt

oder vollstreckbar werden [dürfen], wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.“

Mit freundlichen Grüßen

Johannes Rauch

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2024-08-13T10:32:29+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2098721075
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: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-13T10:37:38+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	