Bundesministerium
Justiz

bmj.gv.at

Dr.in Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2024-0.444.073

Ihr Zeichen: BKA - PDion (PDion)18890/J-NR/2024

Wien, am 13. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Christian Hafenecker, MA, Kolleginnen und Kollegen haben am 13. Juni 2024 unter der Nr. **18890/J-NR/2024** an mich eine schriftliche parlamentarische Anfrage betreffend „Wie steht es um die Datensicherheit des Bundes?“ gerichtet.

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

Zu den Fragen 1 und 3:

- *1. 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)?
- *3. 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 zu PA 18818/J vom 12.06.2024 (XXVII. GP) verwiesen werden.

Zur Frage 2:

- *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 Justiz zeichnet die Abteilung III 3 Rechtsinformatik, Informations- und Kommunikationstechnologie für die IT-Sicherheit verantwortlich. Relevante Informationen fließen in das durch den gemäß NISG eingerichteten IKDOK (Innerer Kreis der Operativen Koordinierung), welcher das gesamtstaatliche Lagebild erstellt.

Zur 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 IT-Leistungen bedient sich das Bundesministerium für Justiz vorrangig der Bundesrechenzentrums GmbH (BRZG) und BBG-gelisteter Produkte und Dienstleistungen. Nicht derartig beschaffbare Leistungen werden gemäß Bundesvergabegesetz und unter Einhaltung der entsprechenden gesetzlichen Rahmenbedingungen (wie zB Verordnung [EU] 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [DSGVO], ABl. Nr. L 119 vom 04.05.2016 S. 1) beschafft.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystem-sicherheitsgesetz, 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.

Zu den Fragen 5 bis 7:

- *5. Wo und wie werden digital generierte Daten (personenbezogene wie nicht-personenbezogene) 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?

- *6. 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)?
- *7. Welche konkreten Maßnahmen und Sicherheitsstrategien verfolgt Ihr Ressort, um möglichen Missbrauch mit Daten durch Dritte zu verhindern?*

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

Zur 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 Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) bzw. die Operativen Koordinierungsstruktur (OpKoord), sowie der Austrian Trust Circle Government (ATC-Gov).

Das durch den IKDOK erstellte Cyberlagebild wird allen Ministerien zur Verfügung gestellt.

Zu den Fragen 9 und 10:

- *9. Wie ist der Stand der NIS-Richtlinien-Umsetzung in Ihrem Ministerium?*
- *10.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 Bundesministerium für Justiz hat die Maßnahmen für die sie betreffenden Bereiche umgesetzt.

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

Zu den Fragen 11 bis 13:

- *11.Gibt es Anstrengungen, Vorhaben oder Überlegungen, die Datenverarbeitung seitens der Bundesverwaltung in Österreich zu bewerkstelligen?*
- *12.Welche Datenarchive im Wirkungsbereich des Bundes liegen im Ausland (Bitte um Auflistung)?*
- *13.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 in den Ministerien erfolgt 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.

Zur Frage 14:

- *Welche Position nimmt die Bundesregierung zum US-„Cloud Act“ in Hinblick auf die DSGVO ein?*

1. Die horizontale Beurteilung von Rechtsvorschriften von Drittländern im Lichte von Unionsrechtsvorschriften (hier: des US-„Cloud Act“ in Hinblick auf die DSGVO) fällt nicht in den Wirkungsbereich des Bundesministeriums für Justiz.

Diesbezüglich wird allgemein auf die Befugnis der Europäischen Kommission zum Erlass von Durchführungsrechtsakten, mit denen beschlossen wird, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet (Art. 45 iVm Art. 92 DSGVO; sog. „Angemessenheitsbeschlüsse“), sowie fallbezogen auf den für die USA bestehenden Angemessenheitsbeschluss (Durchführungsbeschluss der Kommission vom 10.7.2023 gemäß der Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, C(2023) 4745 final) hingewiesen.

2. 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 Drittlandsbezugs (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.“

Dr.in Alma Zadić, LL.M.

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2024-08-13T13:01:35+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	2024-08-13T13:07:13+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	