Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

Mag. Werner Kogler
Vizekanzler
Bundesminister für Kunst, Kultur,
öffentlichen Dienst und Sport

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.450.087

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. 18860/J** 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:

- *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)?*

Ich darf auf meine Beantwortung der parlamentarischen Anfrage Nr. 18817/J betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ verweisen.

Zu 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?*

Die zentrale Stelle in meinem Ressort bildet die Abteilung I/A/8 für Projektmanagement, Digitalisierung und Services.

Zu 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 Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS) vorrangig der BRZ GmbH und BBG-gelisteter Produkte und Dienstleistungen. Nicht derartig beschaffbare Leistungen werden gemäß Bundesvergabegesetz 2018 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 (NISG), 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 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 BMKÖS stellt sicher, dass der Schutz der Daten entsprechend ihrer Sensibilität erfolgt. Daten, die als besonders schützenswert gelten, werden entsprechend gesichert. Mit der BRZ GmbH als zentralem IKT-Dienstleister ist die entsprechende Datensicherheit gewährleistet. Die BRZ GmbH unterzieht sich regelmäßig zu Datenschutz und Sicherheit einem ISO-Audit. Darüber hinaus gibt es zu den diversen Szenarien Notfallpläne, Handlungsanweisungen sowie Kommunikationspläne.

Der Zugang zu den Daten ist je nach deren Sensibilität auf bestimmte Personengruppen beschränkt, um eine maximale Sicherheit und Integrität der Daten zu gewährleisten.

Zu Frage 7:

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

Das BMKÖS stellt sicher, dass der Schutz der Daten entsprechend ihrer Sensibilität erfolgt. Mit dem BRZ als zentralem IT-Dienstleister ist sichergestellt, dass die Maßnahmen dem Stand der Technik entsprechen.

Zu 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 Cyber Security gibt es sowohl auf strategischer, operativer als auch technischer Ebene interministerielle Arbeits- und Austauschgruppen. Als Beispiel kann hier der ressortübergreifende Austausch der IKT-Sicherheitsbeauftragten genannt werden. Das durch den inneren Kreis der operativen Koordinierungsstruktur (IKDOK) erstellte Cyberlagebild wird allen Ministerien zur Verfügung gestellt.

Zu den 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 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 BMKÖS ist bestrebt, die gemäß § 22 NISG geforderten Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen der öffentlichen Verwaltung umzusetzen.

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:

- *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 in den Bundesministerien erfolgt nach Analyse hinsichtlich der Klassifizierung, Kritikalität, Verfügbarkeitsanforderungen und Datenschutzanforderungen abgestuft lokal, auf hausinterner 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 BRZ GmbH wurde ein gesetzlicher Dienstleister eingerichtet, welcher im 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.

Zu 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 ebendieser 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 „jegliches 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.“ Der Abschluss derartiger Rechtshilfeabkommen obliegt den zuständigen Fachministerien.

Mag. Werner Kogler

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR KUNST, KULTUR, ÖFFENTLICHEN DIENST UND SPORT
AMTSSIGNATUR

Unterzeichner	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
Datum/Zeit	2024-08-13T13:38:40+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.	2099471880
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-13T13:44:54+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	