

ANFRAGE

der Abgeordneten Mag. Katayun Pracher-Hilander
an den Bundesminister für Finanzen
betreffend **Internationale Auftragsverarbeiter und Datensicherheit bei der Bundesrechenzentrum GmbH**

Die Bundesrechenzentrum GmbH (BRZ GmbH) fungiert als zentraler IT-Dienstleister und digitaler Knotenpunkt der Republik Österreich. In ihren Rechenzentren und IT-Systemen werden täglich hochsensible Finanz-, Personal-, Gesundheits- und Verwaltungsdaten von Millionen österreichischen Bürgern sowie Unternehmen verarbeitet. Die Gewährleistung uneingeschränkter Datenhoheit, digitaler Souveränität und höchster IT-Sicherheitsstandards stellt daher eine fundamentale Verpflichtung des Bundes gegenüber der Bevölkerung und dem Wirtschaftsstandort Österreich dar.

Aus den aktuellen Datenschutzhinweisen der BRZ GmbH vom November 2025 geht unter Punkt 1.3 hervor, dass sich das Unternehmen zur Datenverarbeitung externer Dienstleister als Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO bedient.¹

Konkret genannt werden Google Inc. mit Sitz in den USA zur Einbindung von Google reCAPTCHA² und YouTube sowie die Microsoft Corporation zur Abwicklung von Online-Meetings über „Teams“³.

Darüber hinaus bleiben die Identität, der Sitz und der konkrete Tätigkeitsumfang weiterer Auftragsverarbeiter jedoch weitgehend unbestimmt. Insbesondere ist nicht ersichtlich, mit welchen weiteren Unternehmen Vertragsbeziehungen bestehen, in welchen Staaten und an welchen Standorten Daten verarbeitet oder gespeichert werden, welche Datenkategorien davon betroffen sind und welche konkreten Sicherheitsmaßnahmen und Verschlüsselungstechnologien dabei zum Einsatz kommen.

Diese mangelnde Transparenz ist insbesondere bei der Einbindung von Dienstleistern aus Drittstaaten problematisch. Ausländische Rechtsvorschriften wie der US CLOUD Act⁴ können den Zugriff ausländischer Behörden auf Daten ermöglichen, die von Unternehmen im jeweiligen Rechtsraum kontrolliert werden. Eine Abhängigkeit des zentralen IT-Dienstleisters der Republik von außereuropäischen Technologiekonzernen birgt daher erhebliche Risiken für die österreichische Datensouveränität und die Unabhängigkeit der staatlichen IT-Infrastruktur.

Zusätzlich stellt die fortschreitende Entwicklung leistungsfähiger Quantencomputer die Sicherheit herkömmlicher kryptografischer Verfahren zunehmend infrage. Vor diesem Hintergrund ist zu klären, welche Maßnahmen die BRZ GmbH zur Umstellung auf quantenresistente Verschlüsselungsverfahren beziehungsweise auf Post-Quanten-Kryptografie bereits getroffen hat und nach welchem Zeitplan die erforderliche Migration erfolgen soll.

¹ <https://www.brz.gv.at/dam/jcr:fd41b849-1147-4c90-8b5b-2a14bbfc38c9/2025.11.13%20-%20Datenschutzzerkl%C3%A4rung%20Allgemein.pdf> , S. 4 (aufgerufen am 21.09.2026)

² Ebd. S. 8.

³ Ebd. S. 14.

⁴ <https://www.congress.gov/bill/115th-congress/house-bill/4943> (aufgerufen am 21.09.2026)

Umfassende Auskünfte über sämtliche Auftragsverarbeiter und Vertragsbeziehungen, die jeweiligen Verarbeitungs- und Speicherorte, die eingesetzten Sicherheitstechnologien sowie insbesondere die Quantenresistenz der Systeme sind im Interesse der parlamentarischen Kontrolle, der digitalen Souveränität Österreichs und der Transparenz gegenüber den Bürgern unerlässlich.

In diesem Zusammenhang richtet die unterfertigte Abgeordnete an den Bundesminister für Finanzen nachstehende

Anfrage

1. Welche externen Dienstleister fungieren derzeit als Auftragsverarbeiter für Verarbeitungstätigkeiten, bei denen die BRZ GmbH selbst datenschutzrechtlich Verantwortlicher ist?
 - a. Wie lauten die genauen Firmennamen und Registrierungsnummern dieser Unternehmen?
 - b. In welchen Staaten haben diese Auftragsverarbeiter ihren satzungsmäßigen Hauptsitz sowie ihre tatsächliche Hauptverwaltung?
 - c. Welche konkreten Datenarten bzw. Datenverarbeitungstätigkeiten werden jeweils an diese Auftragsverarbeiter ausgelagert?
 - d. In welchen Staaten bzw. an welchen physischen Serverstandorten erfolgt die Speicherung und Verarbeitung der jeweiligen Daten durch diese Unternehmen?
2. Welche externen Dienstleister fungieren derzeit als Subauftragsverarbeiter bei Verarbeitungstätigkeiten, welche die BRZ GmbH im Auftrag von Bundesministerien oder sonstigen öffentlichen Stellen durchführt?
 - a. Wie lauten die genauen Firmennamen und Registrierungsnummern dieser Unternehmen?
 - b. In welchen Staaten haben diese Subauftragsverarbeiter ihren satzungsmäßigen Hauptsitz sowie ihre tatsächliche Hauptverwaltung?
 - c. Welche konkreten Datenarten bzw. Datenverarbeitungstätigkeiten werden jeweils an diese Auftragsverarbeiter ausgelagert?
 - d. In welchen Staaten bzw. an welchen physischen Serverstandorten erfolgt die Speicherung und Verarbeitung der jeweiligen Daten durch diese Unternehmen?
3. Mit welchen weiteren IT-Dienstleistern, Hard- und Softwareherstellern sowie Beratungsunternehmen mit Sitz außerhalb Österreichs unterhält die BRZ GmbH derzeit laufende Vertragsbeziehungen?
4. Welche Verschlüsselungstechnologien und Sicherheitsstandards kommen bei der BRZ GmbH derzeit zum Schutz der von ihr selbst oder im Auftrag von Bundesministerien und sonstigen öffentlichen Stellen verarbeiteten Daten bei der Übertragung („Data in Transit“), der Speicherung („Data at Rest“) und der laufenden Verarbeitung („Data in Use“) zum Einsatz?
5. Welche konkrete Strategie verfolgt die BRZ GmbH im Hinblick auf die Bedrohung durch künftige Quantencomputer?
6. Existiert im Bundesministerium für Finanzen bzw. in der BRZ GmbH ein konkreter Zeit- und Finanzierungsplan zur Ertüchtigung der staatlichen Rechenzentrums- und Verschlüsselungsinfrastruktur gegen quantencomputer-gestützte Angriffe?

- a. Welche Budgetmittel wurden hierfür bereitgestellt? (Bitte um Aufschlüsselung nach Jahren ab 2015)
 - b. Welche Mittel sind für diese Legislaturperiode vorgesehen?
7. In welchem Ausmaß und in welchen konkreten Aufgabenbereichen bedient sich die Land-, forst- und wasserwirtschaftliches Rechenzentrum GmbH (LFRZ GmbH) als 100%-Tochter der BRZ GmbH externer Subauftragsverarbeiter mit Sitz im Ausland?

Prache-Silano
Bayer Ricarda

