4636/AB
vom 05.05.2026 zu 5223/J (XXVIII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Christian Stocker
Bundeskanzler

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2026-0.218.935

Wien, am 5. Mai 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dipl.-Ing. Deimek, Kolleginnen und Kollegen haben am 10. März 2026 unter der Nr. **5223/J** eine schriftliche parlamentarische Anfrage betreffend „Härte in der Forderung – Schwäche im Vollzug: ID Austria ohne robuste Korrekturketten – Fehlzuordnungen zu Lasten Unbeteiligter, Verantwortlichkeiten, Kennzahlen, Audits und Maßnahmenplan“ an mich gerichtet.

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

Zu Frage 1:

1. *Welche Organisationseinheiten im Bundeskanzleramt sind für ID Austria fachlich und operativ zuständig? (Bitte um Angaben zu Abteilung/Gruppe, Aufgaben, Personalressourcen)*

Ich verweise auf die Geschäftseinteilung des Bundeskanzleramtes, welche im Internet öffentlich einsehbar ist.

Zu den Fragen 2, 4, 6, 7, 9, 10, 16, 17, 19 bis 23 und 29 bis 32:

2. *Welche ressortübergreifende Governance besteht für das Zusammenspiel von ID Austria mit registerbasierten Verfahren (insbesondere ZMR/Meldewesen, finanzielle Verfahren, gewerbliche Verfahren)?*
   a. *Wer führt den Vorsitz?*
   b. *Wie oft tagt diese Struktur seit 2023?*
   c. *Welche verbindlichen Outputs (Standards, Beschlüsse, Roadmaps) wurden beschlossen?*
4. *Welche Eskalations- und Entscheidungslogik gilt, wenn ein ressortübergreifender „Case" (Fehlzuordnung) im Vollzug feststeckt? (Bitte um Darstellung der Eskalationsstufen und Zuständigkeiten)*
6. *Wie viele Support-/Beschwerdefälle beim Digitalen Amt / ID-Austria gab es 2022, 2023, 2024 und 2025 insgesamt und nach Hauptkategorien (je Jahr)?*
7. *Wie viele dieser Fälle betrafen „Fehlzuordnung/Adress-/Identitätsprobleme mit Drittbetroffenheit"? (Bitte um Aufschlüsselung nach Jahren für 2022-2025)*
   1. *Wenn keine Kategorie existiert, warum nicht?*
   2. *Wenn keine Kategorie existiert, wird sie eingeführt?*
9. *Wie viele Fälle mussten vom BKA an andere Stellen (z. B. BMI/Meldebehörde, BMF, andere) eskaliert werden? (Bitte um Aufschlüsselung nach Jahr und Empfängerkategorie)*
10. *Wie viele eskalierte Fälle wurden end-to-end geschlossen und welche mediane end-to-end-Dauer ergab sich (Bitte um Aufschlüsselung nach Jahr)*
    1. *Wenn keine Erfassung erfolgt, warum nicht?*
16. *Welche standardisierte Korrektur- und Entlastungskette gibt es für unbeteiligte Bürger, die durch Fehlzuordnung belastet werden (One-Stop-Logik: Kontaktpunkt, Fallnummer, end-to-end-Verantwortung)?*
17. *Gibt es eine übergreifende Vorgangs-ID/Fallnummer, die ressortübergreifend genutzt wird?*
    a. *Wenn ja, wie ist sie implementiert?*
    b. *Wenn nein, ist die Einführung geplant (Zeitplan)?*
19. *Welche Ist-Zeiten (Median/90. Perzentil) wurden 2022–2025 tatsächlich erreicht? (Bitte um Aufschlüsselung nach Jahr)*
20. *Welche Möglichkeiten bestehen für Betroffene, Folgewirkungen bis zur Bereinigung zu minimieren (z. B. Deaktivierung bestimmter Zustellwege, Flag an angebundene Stellen)?*

21. *In welchen Verwaltungsprozessen ist ID Austria faktisch Zugangsvoraussetzung oder führt Nichtnutzung zu wesentlichen Nachteilen? (Bitte um Darstellung nach Verfahrensarten)*
22. *Welche analogen Alternativen bestehen pro Verfahrensart (inkl. Fristen, Gebühren, Bearbeitungszeiten) und wie wird Gleichwertigkeit sichergestellt?*
23. *Welche Risikoabwägung nimmt die Bundesregierung vor, wenn Nutzung forciert wird, aber Fehlzuordnungen Dritte belasten können? (Bitte um Darstellung von dokumentierten Risikoanalysen/Entscheidungsgrundlagen)*
29. *Welche verbindlichen Schnittstellen-/Datenqualitätsanforderungen wurden mit dem BMI (ZMR/Meldewesen) festgelegt? (Bitte um Darstellung der Inhalte und des Umsetzungsstands)*
30. *Welche Mechanismen bestehen, damit Korrekturen end-to-end in angebundenen Systemen wirksam werden (Push/Pull, Benachrichtigung, Fristen)?*
31. *Welche Hindernisse verhindern derzeit, dass eine Korrektur „alle Folgesysteme heilt“? (Bitte um Darstellung der Top-Hürden und des Abhilfeplans)*
32. *Welche konkreten kurzfristigen (0-6 Monate), mittelfristigen (6-18 Monate) und langfristigen (18+ Monate) Maßnahmen werden zur Prozesshärtung umgesetzt? (Bitte um Darstellung mit Verantwortlichkeiten, Meilensteinen)*

Das Bundeskanzleramt stellt entsprechend den einschlägigen Bestimmungen des E-Government-Gesetzes insbesondere das System ID Austria zur Identifizierung und Authentifizierung von E-ID-Inhabern zur Verfügung. Ob ein registerführender Verantwortlicher des öffentlichen oder privaten Bereichs die Entscheidung trifft, eine E-ID-taugliche Umgebung einzurichten und „registerbasierte Verfahren“ einzusetzen bzw. zur Verfügung zu stellen, unterliegt als dessen autonome Entscheidung nicht der Zuständigkeit des Bundeskanzleramt.

Neben dem Bundeskanzleramt nimmt auch das Bundesministerium für Inneres wesentliche Aufgaben im Zusammenhang mit dem System ID Austria wahr. Insbesondere anzuführen sind:

- Registrierung der Funktion E-ID für Staatsbürger und Fremde gemäß § 4a E-GovG
- Verarbeitung der Registrierungsdaten zu Zwecken der Verwaltung des E-ID gemäß § 4b Abs 1 E-GovG
- Registrierung und Akkreditierung von privaten Dritten, die das System ID Austria als sogenannte Service Provider nutzen wollen, gemäß § 18 Abs 2 und 3 sowie 5 bis 7 E-GovG

- Funktion als Auftragsverarbeiter für die Stammzahlenregisterbehörde bei der Führung des Ergänzungsregisters, der Errechnung von Stammzahlen und der Durchführung der in den §§ 4, 4b, 5, 9, 10, 14, 14a und 15 E-GovG geregelten Verfahren, soweit natürliche Personen betroffen sind, gemäß § 7 Abs 2 E-GovG

In den Jahren 2022 bis 2025 wurde in diesem Zusammenhang jeweils die folgende Anzahl an Supportfällen im Service Center der ID Austria registriert; eine Erfassung in Kategorien erfolgt nicht:

Jahr	Anzahl der Supportfälle
2022	72.435
2023	103.191
2024	186.543
2025	262.081

Zu Frage 3

3. *Welche verbindlichen Prozess-/Qualitätsstandards (z. B. „first-time-right“, Korrekturfristen, Audit-Trail-Mindestanforderungen) gelten für das Digitale Amt im Betrieb?*

Die App "Digitales Amt" gibt es seit 20. Juni 2025 nicht mehr.

Zu Frage 5:

5. *Welche KPIs werden für ID Austria im Regelbetrieb gemessen (z. B. Verfügbarkeit, Abbruchraten, Fehlermeldungen, Supporttickets, Zeit bis Lösung) und welche Zielwerte gelten?*

Gemessen werden die E2E Verfügbarkeit sowie die Verfügbarkeit des E-ID Frontends für welches eine vertragliche Verfügbarkeit von 99% gewährleistet wird.

Darüber hinaus gibt es erweiterte Statistiken zur Anzahl der Anmeldungen am E-ID System, Anzahl der ID-Austria Registrierungen, Anzahl aktiver ID Austria Konten sowie Anzahl der ID Austria Service Provider.

Zu Frage 8:

8. *Welche mediane Bearbeitungszeit und welches 90. Perzentil bestehen bei Supportfällen insgesamt sowie bei der Kategorie „Fehlzuordnung/Adress-/Identitätsprobleme“ (je Jahr 2022–2025)?*

Darüber werden keine Aufzeichnungen geführt.

Zu den Fragen 11 bis 13, 15 und 18:

11. *Welche konkreten Prüfschritte sind im Digitales-Amt-Kontext vorgesehen, um Missbrauch oder Fehlzuordnungen zu erkennen, bevor Folgewirkungen eintreten?*
12. *Welche Plausibilitätsprüfungen bestehen im Zusammenspiel mit Registerdaten, um unplausible Konstellationen zu erkennen (z. B. massenhafte Vorgänge, ungewöhnliche Häufungen, Fluktuation)?*
13. *Gibt es eine automatisierte Anomalie-/Fraud-Erkennung (regelbasiert oder datengetrieben) im Kontext Digitales Amt I ID-Austria (in zusammenfassender Form)?*
    a. *Wenn ja, welche Grundlogik und Governance (Freigabe/Monitoring) liegt zugrunde?*
    b. *Wenn nein, warum nicht?*
15. *Welche Maßnahmen bestehen, um kompromittierte Zugänge bzw. Identitätsmissbrauch rasch zu erkennen und zu stoppen (Sperre, Flag, Wiederherstellung, Meldelogik)?*
18. *Welche verbindlichen Fristen gelten für*
    a. *Erstreaktion/Erstprüfung,*
    b. *vorläufige Sicherungsmaßnahmen (Flag/Sperre),*
    c. *endgültige Bereinigung?*

Im Kontext des E-ID ist auf die einschlägigen gesetzlichen Bestimmungen der §§ 8 ff E-GovG zu verweisen, insbesondere betreffend die eindeutige Identifikation in Datenverarbeitungen, den Schutz der Stammzahl natürlicher Personen sowie weitere Garantien zum Schutz von Bereichsspezifischen Personenkennzeichen (bPK) .

Zu Frage 14:

14. *Welche Protokollierung/Audit-Trail-Standards gelten (Wer hat wann was ausgelöst), und welche Aufbewahrungsfristen gelten (bitte systematisch darstellen)?*

Ich verweise insbesondere auf das Kapitel 4.6. der im Internet unter https://www.id-austria.gv.at/dam/jcr:040bc953-08b7-4b62-af9c-92ccfabdbcb3/DSFA-ID_Austria-20250603.pdf veröffentlichten „ID Austria Datenschutz-Folgenabschätzung“.

Zu Frage 24:

24. Wurden seit 2022 Sicherheits- und Prozess-Audits für ID Austria durchgeführt? (Bitte um Aufschlüsselung nach Anzahl, Zeitpunkt, Prüfumfang je Audit)

a. Wenn ja, wie ist der Umsetzungsstatus der abgeleiteten Maßnahmen?

Es werden regelmäßig Sicherheits PEN-Tests im Rahmen der ID Austria durchgeführt, um mögliche Schwachstellen aufzuspüren, diese nach dem Risikopotential zu bewerten und zu beheben. Folgende PEN Tests wurden seit 2022 durchgeführt:

- 2022: Sicherheitstest ID Austria Frontend (Der Hauptfokus des Tests lag in einem Nachfolgetest aller Schwachstellen, welche bisher in verschiedenen vorherigen Projekten aufgedeckt wurden. Zusätzlich wurde ein Schwerpunkt auf die Applikation der Service-Provider-Registrierung gelegt, welche seit der letzten Prüfung größeren Änderungen unterlegen war).
- 2023: Sicherheitstest Digitale Amt App (Es wurde ein externer Grey-Penetrationstest der „Digitales Amt“ App mit Fokus auf die Funktion „Signatur-Passwort zurücksetzen“ durchgeführt).
- 2024: PEN Test des bilateralen Vertretungsregister der ID Austria
- 2024: PEN Test ID Austria Frontend (wurde ein Whitebox Penetrationstest auf die gesamten BRZ Frontend Komponenten durchgeführt, bei dem ein Hacking-Angriff simuliert wurde)
- 2024: PEN Test der neuen ID Austria App – Teil 1
- 2025: PEN Test der neuen ID Austria App – Teil 2

Es gibt keine dedizierten Prozessaudits für ID Austria. Diese finden auf Unternehmensebene statt. Das BRZ ist zertifiziert nach ISO 27001 (Informationssicherheits-Managementsystem), ISO 22301 (Business Continuity). Darüber hinaus setzt die BRZ GmbH über 250 Grundschutzmaßnahmen in den Bereichen Objekt- und Zutrittsschutz, personelle Sicherheit, Server und Datenbanken, Datenspeicher, Software und EDV-Anwendungen ein.

Darüber hinaus verweise ich auf https://www.brz.gv.at/was-wir-tun/zertifizierungen.html.

Zu Frage 25:

25. Wurden Datenschutz-Folgenabschätzungen (DSFA) für kritische Prozessketten erstellt, die Drittbetroffenheit erzeugen können?

a. Wenn ja, welche Ketten, welche Risikominderungen (zusammenfassend, nicht sicherheitsgefährdend) gibt es?

b. Wenn nein, warum nicht?

Zur ID Austria wurden 2022 als auch 2025 umfangreiche Datenschutz-Folgenabschätzungen durchgeführt und die gemeinsam mit externen Datenschutzexperten erstellten zugehörigen Berichte veröffentlicht. Siehe dazu nachstehenden Link: https://www.id-austria.gv.at/dam/jcr:040bc953-08b7-4b62-af9c-92ccfabdbcb3/DSFA-ID_Austria-20250603….

Zu Frage 26:

26. Welche Qualitätsmanagement-Mechanismen bestehen (Release-Gates, Incident-Postmortems, „Stop-the-line" bei systemischen Fehlern)?

Das Qualitätsmanagement ist auf BRZ Unternehmensebene standardisiert.

Das Qualitätsmanagement des BRZ erfolgt prozessorientiert und auf Grundlage der Anforderungen der ISO9001. Das BRZ ist seit dem Jahr 2003 ISO9001 zertifiziert, das Qualitätsmanagement-System somit durch eine unabhängige dritte Stelle auf Funktionsfähigkeit und Wirksamkeit überprüft. Sämtliche Prozesse, Abläufe, Verfahren, Instrumente, Strukturen, usw. müssen somit regelmäßig einem Review unterzogen und gegebenenfalls angepasst werden. Die BRZ Management Practices orientieren sich nach ITIL Practices und umfassen Standards für:

1. Incident Management: Wiederherstellung des normalen Servicebetriebs
2. Problem Management: Analyse von Ursachen für Incidents
3. Change Enablement (Change Management): Risikominimierung bei Änderungen
4. Service Desk: Zentrale Anlaufstelle für Anwender
5. Service Level Management: Definition und Überwachung von Servicezielen (SLAs)
6. IT Asset Management / CMDB: Verwaltung von IT-Komponenten

Standardisierte Quality Gates and Checks beim Release von Softwarekomponente und Service garantieren die Qualitätssicherung.

Zu den Fragen 27 und 28:

27. Welche Gesamtaufwendungen (IT, Betrieb, Support, Weiterentwicklung, externe Leistungen) entfielen 2022–2025 auf ID Austria? (Bitte um Aufschlüsselung nach Jahr und Kostenarten)

28. Welche Budgets/Planstellen sind 2026/2027 für Prozesshärtung, Support und Korrekturketten vorgesehen?

Kostenart	Jahr

	2022	2023	2024	2025
ID Austria Betrieb inkl. Support	3.716.787,86	6.385.613,69	7.150.071,39	8.382.469,77
Weiterentwicklung	619.219,86	3.724.819,47	3.323.671,65	1.643.947,16
Externe Leistungen	209.032,32	121.622,40	572.193,69	579.517,15
Begleitmaßnahmen zur Einführung und Verbreitung	110.500,3	1.925.850,64	137.594,54	73.036,34

Eine darüberhinausgehende Aufschlüsselung kann nicht erfolgen.

Zu Frage 33:

33. Prüft das BKA eine gesetzliche oder organisatorische Systemänderung („Ein Fall – eine Lösung“ mit verbindlichen Fristen und Durchgriff)?

a. Wenn ja, welche Optionen werden geprüft und mit welchem Zeitplan?

b. Wenn nein, warum nicht?

Gesetzliche und organisatorische Anpassungen werden aufgrund der Umsetzung der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität erforderlich.

Zu Frage 34:

34. Welche messbaren Zielgrößen werden 2026/2027 angestrebt (z. B. Zeit bis Case-Closure, Quote wiederkehrender Fehlzuordnungen, Support-SLAErfüllung)?

Das BRZ garantiert die vertraglich vereinbarte Verfügbarkeit mit SLA von 99% für die von ihm betriebenen ID Austria Komponenten.

Dr. Christian Stocker

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2026-05-05T16:37:27+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2026-05-05T17:29:40+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	