10037/AB
vom 23.05.2022 zu 10280/J (XXVII. GP)

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

bmdw.gv.at

Univ.-Prof. Dr. Martin Kocher
Bundesminister für Digitalisierung und Wirtschaftsstandort

Stubenring 1, 1010 Wien

Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.226.437

Ihr Zeichen: E-Mail

In Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 10280/J betreffend "ID Austria", welche die Abgeordneten Katharina Kucharowits, Kolleginnen und Kollegen am 23. März 2022 an meine Amtsvorgängerin richteten, stelle ich fest:

Antwort zu Punkt 1 der Anfrage:

1. *Welche konkreten Funktionen wird die künftige ID Austria haben? Bitte um Auflistung aller Funktionen.*

Die ID Austria ist technisch gesehen ein Identity Provider (IDP), der Attribute von Bürgerinnen und Bürgern an öffentliche und private Service Provider (Applikationen) ausliefern kann. Aktuell handelt es sich dabei um das sogenannte Minimum Data Set (MDS): Name, Geburtsdatum und bereichsspezifisches Personenkennzeichen (bPK) für die eindeutige Identifikation anhand des bPK-Konzepts. Weitere Attribute sind geplant. Für die Auslieferung der Daten werden die als weltweiter Standard eingesetzten Protokolle SAML/OIDC verwendet.

Damit ein öffentlicher oder privater Service Provider ID Austria als Identity Provider verwenden kann, muss die jeweilige Applikation im Service-Provider-Register registriert sein. Private Service Provider müssen akkreditiert werden, damit sichergestellt ist, dass die rechtlichen Rahmenbedingungen eingehalten werden; so etwa die Frage, ob ein Attribut an den gegeben Service Provider ausgeliefert werden darf.

Die Anmeldung einer Bürgerin oder eines Bürgers bei einem Service Provider kann also nur erfolgen, wenn der Service Provider korrekt registriert wurde. Zusätzlich wird die Bürgerin oder der Bürger darüber informiert, welche Attribute an den Service Provider einmalig übermittelt werden; jede weitere Übermittlung erfordert auch eine weitere Anmeldung. Je nach rechtlichem Rahmen ist dies als reine Information oder als datenschutzrechtliche Einwilligung, die für die Übermittlung benötigt wird, anzusehen. Bei privaten Service Providern ist für alle Attribute außer dem bPK eine datenschutzrechtliche Einwilligung erforderlich.

Da die Anmeldung über die Erstellung der qualifizierten Signatur durchgeführt wird, steht automatisch jeder Bürgerin und jedem Bürger auch die elektronische qualifizierte Unterschrift unabhängig von der Verwendung von ID Austria zur Verfügung.

In Zukunft sollen weitere Attribute und Use Cases aus dem privaten und öffentlichen Bereich ergänzt werden.

Antwort zu Punkt 2 der Anfrage:

2. Welche konkreten Funktionen wird die künftige Ausweisplattform haben? Bitte um Auflistung aller Funktionen.

Als erster Ausweis wird der digitale Führerschein zur Verfügung stehen. Dieser kann sowohl im Rahmen einer Verkehrskontrolle wie auch für den Nachweis der Lenkberechtigung gegenüber einer anderen Bürgerin und einem anderen Bürger oder einem Unternehmen verwendet werden. Für den Zulassungsschein wird schon eine mögliche Umsetzung analysiert. Auch werden bereits weitere potentiell in Frage kommende Ausweise auf Bundes- und Landesebene sowie für Anforderungen der Privatwirtschaft analysiert.

Antwort zu den Punkten 3, 5, 10 und 23 der Anfrage:

3. Welche(s) Unternehmen wurde(n) bzw. wird/werden mit der Entwicklung und Programmierung von ID Austria beauftragt?
5. Welche Kosten sind für die Entwicklung und Programmierung der ID Austria bislang angefallen?
10. Greift ID Austria auf die Nutzung, Speicherung oder Weitergabe von biometrischen Daten des Endgeräts, etwa Gesichtserkennung oder Fingerabdrucksensor, zu?
    a. Falls ja, wozu greift ID Austria konkret auf biometrische Daten zu? Zu welchen Funktionen benötigt die Anwendung den Zugriff?

*b. Falls ja, wie werden diese hochsensiblen Daten von Nutzer*innen vor einer rechtswidrigen Verwendung, Speicherung oder Weitergabe durch Behörden oder Dritte geschützt?*

c. Falls ja, ist die Verwendung von ID Austria auch ohne Verwendung biometrischer Daten möglich?

23. Werden jene Menschen, die bereits die Handysignatur nutzen, automatisch in die ID Austria überführt?

a. Wenn ja, wann und wie konkret?

*b. Falls nein, können diese Nutzer*innen die ID Austria online beantragen oder ist ein physischer Weg zu den Behörden/auf das zuständige Amt nötig?*

Dazu ist auf die Beantwortung der parlamentarischen Anfrage Nr. 10222/J zu verweisen.

Antwort zu Punkt 4 der Anfrage:

4. Welche(s) Unternehmen wird/werden mit der (laufenden) Wartung von ID Austria beauftragt?

Mit dem Betrieb der ID Austria wird die BRZ GmbH beauftragt; die Wartungskosten sind Bestandteil des Betriebsvertrages.

Antwort zu Punkt 6 der Anfrage:

6. Welche Kosten sind für die Entwicklung der Ausweisplattform durch die Staatsdruckerei kalkuliert?

Die Entwicklung der generischen Ausweisplattform wurde bei der ARGE youniqx Identity AG beauftragt; die vorgesehenen Kosten dafür betragen € 281.808,00.

Antwort zu Punkt 7 der Anfrage:

7. Welche Kosten sind für die laufende Wartung von ID Austria einerseits und die Ausweisplattform andererseits bisweilen angefallen bzw. welche Höhe an Kosten ist zu erwarten?

Die Wartungskosten für die ID Austria sind im Betriebsvertrag inkludiert und können nicht gesondert ausgewiesen werden. Da sich die Ausweisplattform noch nicht in Betrieb befin-

det, fallen derzeit noch keine Wartungskosten an. Die Wartungskosten werden auch in diesem Fall Bestandteil des Betriebsvertrages sein.

Antwort zu Punkt 8 der Anfrage:

*8. Welche (personenbezogenen) Daten von Nutzer*innen wird ID Austria konkret a) speichern, b) verwenden und/oder c) an Dritte weitergeben? Bitte um detaillierte Auflistung. Und auf welcher gesetzlichen Grundlage basiert all dies?*

Für die Verwaltung und Registrierung der ID Austria sind die Registrierungsbehörden gemäß § 4b Abs. 1 E-Government-Gesetz (E-GovG) ermächtigt, folgende Daten zu verarbeiten:

1. die Namen,
2. das Geburtsdatum,
3. den Geburtsort,
4. das Geschlecht,
5. die Staatsangehörigkeit,
6. das bPK,
7. die bekanntgegebene Zustelladresse,
8. das aktuelle Lichtbild, ausgenommen das Lichtbild eines Reisepasses gemäß § 4a des Passgesetzes 1992
9. das Registrierungsdatum,
10. soweit verfügbar die bekanntgegebene Telefonnummer eines Mobiltelefons,
11. soweit verfügbar die bekanntgegebene E-Mail-Adresse,
12. die Registrierungsbehörde und
13. den Identitätscode der ausgestellten Zertifikate gemäß § 4 Abs. 4 E-GovG

Bei der Verwendung der ID Austria durch die Nutzerin oder den Nutzer werden die Personenidentifikationsdaten (Name, Geburtsdatum und bPK) einer Person verarbeitet, also in die Personenbindung eingefügt und an Service Provider übermittelt. Bei Service Providern aus dem privaten Bereich wird nur das bPK übermittelt. Namen und Geburtsdatum werden an Private nur mit Einwilligung der Userinnen und User übermittelt. Mit Einwilligung der betroffenen Person können auch weitere Merkmale wie etwa Alter, Personenstand oder Lenkerberechtigung aus Datenquellen, die der Stammzahlenregisterbehörde rechtlich und technisch zugänglich sind, in die Personenbindung eingefügt und an Dritte übermittelt werden. Rechtsgrundlage für die Verwendung der ID-Austria sind §§ 4 Abs. 5, 14 Abs. 3 und 14a Abs. 2 E-GovG. Damit ein weiteres Merkmal über die ID Austria ausgelie-

fert werden kann, muss dafür eine entsprechende (materien)rechtliche Grundlage bestehen (vgl. etwa § 15a Führerscheingesetz).

Antwort zu Punkt 9 der Anfrage:

9. Welche privatwirtschaftlichen Unternehmen waren mit dem Ministerium für Digitalisierung und Wirtschaftsstandort über Pläne für die Nutzung der ID Austria bereits in Kontakt?

Es gab bereits Kontakt mit Vertreterinnen und Vertretern unterschiedlicher Branchen, die die Identität ihrer Kundinnen und Kunden auf möglichst sichere Art und Weise online sowie vor Ort prüfen müssen. Dazu zählen Banken und Finanzdienstleister wie Raiffeisenlandesbank NÖ-W, Erste Group, Bawag und Coinfinity, Transportunternehmen wie ÖBB und Wiener Linien, Post AG sowie APA, Monopolverwaltung GmbH, Bau-ID, Gemdat, AN-KÖ und Ö-Ticket.

Antwort zu den Punkten 11 und 12 der Anfrage:

*11. Wo werden die {personenbezogenen) Daten von Nutzer*innen, die ID Austria nutzt, speichert oder weitergibt, gespeichert?*
*12. Wer hat auf die (personenbezogenen) Daten von Nutzer*innen, die ID Austria nutzt, speichert oder weitergibt, Zugriff? Bitte um detaillierte Auflistung aller Zugriffsberechtigten.*

Die Registrierungsdaten sind in der Datenverarbeitung gemäß § 22b Passgesetz 1992 zu verarbeiten. Die Daten von Nutzerinnen und Nutzern, die im Rahmen der E-ID-Verwendung weitergegeben werden, sind in den für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen oder privaten Bereichs gespeichert. Eine zusätzliche Speicherung dieser Daten durch ID Austria erfolgt nicht.

Auf die Protokolldaten gemäß § 18 Abs. 1 letzter Satz E-GovG, welche lediglich die übermittelten Attributskategorien ohne die konkreten Attributwerte beinhalten, hat die Inhaberin oder der Inhaber der ID Austria Zugriff. Weiters gibt es im Rahmen von vom Betroffenen selbst ausgelösten datenschutzrechtlichen Prozessen wie etwa einem Antrag auf Auskunft zu deren Erfüllung Zugriffsmöglichkeiten auf die Protokolldaten für einen eingeschränkten Personenkreis im Bundesministerium für Digitalisierung und Wirtschaftsstandort bzw. der BRZ GmbH als dessen Auftragsverarbeiterin.

Antwort zu den Punkten 13, 14 und 22 der Anfrage:

13. *Mit welchen Maßnahmen sollen die Identitätsdaten der ID Austria vor überschießendem Zugriff durch privatwirtschaftliche Akteur*innen geschützt werden?*
14. *Im Kompromisstext der französischen Ratspräsidentschaft vom 10. März 2022 wird ein erhöhtes Schutzniveau für den Zugriff von Identitätsdaten durch privatwirtschaftliche Akteur*innen vorgeschrieben und damit vom Vorschlag der EU-Kommission abgewichen. Welche parallelen Absicherungen gibt es bei der ID Austria auf technischer und organisatorischer Ebene, um den überschießenden Zugriff auf Identitätsdaten durch die Privatwirtschaft zu verhindern?*
22. *Im Zusammenhang mit der Einführung der ID Austria haben bereits mehrere Expert*innen ihre Bedenken geäußert. So könnten auch Privatunternehmen als Serviceprovider auftreten, nicht nur Behörden. Wird gewährleistet, dass die {personenbezogenen) Daten von Nutzer*innen vor einer missbräuchlichen oder rechtswidrigen Verwendung durch Privatunternehmen geschützt sind?*
    a. *Falls ja, wie sieht dieser Schutz konkret aus?*
    b. *Falls nein, warum nicht?*

Gemäß § 18 E-GovG ist Dritten, das sind im Sinne dieser Bestimmung private Service Provider, die Nutzung des E-ID Systems, also der ID Austria, vom Bundesministerium für Inneres unter den in dieser Bestimmung vorgesehenen Voraussetzungen zu eröffnen. Die Nutzung ist nicht zu eröffnen oder zu unterbinden, wenn Anhaltspunkte dafür bestehen, dass Dritte die ihnen zur Verfügung gestellten personenbezogenen Daten nicht gemäß dem Grundsatz von Treu und Glauben und auf rechtmäßige Weise verarbeitet haben. Weiters haben private Service Provider dem Bundesministerium für Inneres jeden Umstand bekanntzugeben, der einer Nutzung entgegensteht. Die an Dritte (Private) übermittelten personenbezogenen Daten dürfen im konkreten Fall nur für die glaubhaft gemachten eigenen Zwecke verarbeitet werden; die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck im Sinne dieser Bestimmung.

Privatwirtschaftliche Akteure müssen die Anwendungen bei ID Austria registrieren und definieren, welche Attribute sie im Zuge der Anwendung erhalten möchten. Das Bundesministerium für Inneres führt dazu den Akkreditierungsprozess durch und prüft die rechtlichen Rahmenbedingungen. Wenn die Akkreditierung erfolgt ist, kann die Anwendung freigeschaltet werden und Bürgerinnen und Bürger können sich bei der Anwendung mit ID Austria anmelden. Bei der Anmeldung erfolgt die Auflistung der Daten, die einmalig bei diesem Anmeldevorgang an den privaten Service Provider übermittelt werden. Die Bürge-

rin oder der Bürger muss datenschutzrechtlich zu dieser Übermittlung einwilligen. Nach der Anmeldung werden die Daten anhand der technischen Standards SAML/OIDC an den Service Provider übermittelt. Dies erfolgt nur einmalig. Eine weitere Übermittlung kann nur erfolgen, wenn eine neue Einwilligung/Anmeldung der Bürgerin oder des Bürgers erfolgt.

Für die Übermittlung von Daten an privatwirtschaftliche Akteure muss also zuerst die Akkreditierung durchgeführt werden, und danach müssen die Benutzerinnen und Benutzer pro Anmeldevorgang einwilligen, dass eine Übermittlung der jeweiligen Attribute erfolgen kann.

Antwort zu Punkt 15 der Anfrage:

15. *In § 7 der kürzlich erlassenen Stammzahlenregisterverordnung 2022 des Ministeriums für Digitalisierung und Wirtschaftsstandort wird es privatwirtschaftlichen Unternehmungen ermöglicht, bereichsspezifische Personenkennzeichen (bPKs) zu erlangen. Welche Verwendungszwecke sind für diese bPKs vorgesehen?*
    a. *Was wäre aus Sicht des Ministeriums eine widerrechtliche Verwendung dieser bPKs?*
    b. *Welche Branchen sind als legitime Anwender dieser Bestimmung vorgesehen?*
    c. *Welche Maßnahmen zur Absicherung der Verwendung des bPK vor Missbrauch sind vorgesehen?*

Zur Stammzahlenregisterbehördenverordnung 2022 liegt zum Anfragestichtag lediglich ein Begutachtungsentwurf vor. Die Verwendung von bPK im privaten Bereich ist bereits jetzt in § 7 Stammzahlenregisterverordnung 2009 geregelt. Die Ausstattung von privaten Datenverarbeitungen mit bPK erfolgt häufig aufgrund einer unmittelbaren gesetzlichen Meldeverpflichtung, so etwa von Banken im Zusammenhang mit dem Kontenregister oder Spendenorganisationen für die Berücksichtigung von Spenden bei der automatischen Arbeitnehmerveranlagung, wofür auch die Verarbeitung von bPK ausdrücklich normiert ist.

Die bPK dürfen immer nur für den bei der Ausstattung angegeben Zweck verarbeitet werden. Eine zweckwidrige Verarbeitung von personenbezogenen Daten ist nicht zulässig. Für die Errechnung des bPK hat der Verantwortliche der Stammzahlenregisterbehörde seine Stammzahl oder sein bPK zur Verfügung zu stellen. Gemäß § 14 Abs. 2 E-GovG dürfen Verantwortliche des privaten Bereichs nur solche bPK speichern und benützen, die mit Hilfe ihrer eigenen Stammzahl oder ihrem eigenen bPK als Bereichskennung gebildet wurden.

Antwort zu Punkt 16 der Anfrage:

*16. Wie werden die (personenbezogenen) Daten von Nutzer*innen, die ID Austria verwendet, speichert und/oder weitergibt, vor Missbrauch oder bei Diebstahl des Smartphones geschützt?*

Die Daten der Benutzerinnen und Benutzer werden nicht am Smartphone gespeichert, sondern bei jedem Anmeldevorgang von ID Austria bezogen und an den Service Provider übermittelt. Wesentlich ist daher der Schutz der Authentifizierungsmaßnahmen; dazu werden alle Best-Practice Ansätze aus dem Bereich Smartphone-Sicherheit angewendet:

- Technisch:
  - Authentifizierungsmittel: Kryptographische Schlüssel werden nur in den dedizierten Hardware-basierten Schlüsselspeichern der Geräte wie etwa Secure Enclave, Strongbox etc. aufbewahrt. Die Schlüssel können nicht extrahiert, sondern nur verwendet werden, wenn das biometrische Merkmal korrekt vorhanden ist, und können auch nicht auf andere Geräte übertragen werden. Beim Hinzufügen von biometrischen Merkmalen werden die Schlüssel automatisch ungültig und können nicht mehr verwendet werden.
  - Root-Detection: Auf Android-Geräten wird mit mehreren Methoden sichergestellt, dass das Gerät in einem sicheren, nicht gerooteten Zustand ist, das sind einerseits Checks, die nach Merkmalen suchen, die für "gerootete" Geräte typisch sind, andererseits Checks, ob die Sicherheit des Bootloaders gewährleistet ist (key attestation).
  - Einsatz von drei Faktoren: Für eine erfolgreiche Authentifizierung werden die drei Faktoren eingesetzt:
    - Wissen: globales, nicht an das Gerät gebundenes Passwort
    - Besitz: Das Smartphone muss im Besitz sein, da die kryptographischen Schlüssel nur auf einem initialisierten Gerät verwendet und nicht auf andere Geräte übertragen werden können.
    - Biometrische Eigenschaft: Für die Verwendung der kryptographischen Schlüssel wird die biometrische Eigenschaft benötigt. In Zukunft ist hier angedacht, als Alternative einen PIN zu verwenden. Dieser PIN ist auch an das Gerät gebunden und kann nur auf diesem verwendet werden.
- Organisatorisch
  - Deaktivieren von Geräten: Da es auftreten kann, dass bestimmte Geräteklassen schwerwiegende Fehler haben, die die Sicherheit verletzen, werden diese Gerä-

teklassen bei derartigen Mängeln temporär oder permanent deaktiviert, je nachdem, ob die Mängel von den Herstellern behoben werden.

Antwort zu den Punkten 17 und 20 der Anfrage:

17. *Haben Nutzer*innen Einsicht oder Kenntnis darüber, welche ihrer Daten durch ID Austria gespeichert, verwendet oder weitergegeben und an wen sie weitergeben werden?*
    a. *Falls ja, von wem, wodurch und wie detailreich werden Nutzer*innen informiert?*
    b. *Falls nein, warum nicht?*
20. *Werden neben den Daten von Nutzer* innen auch die einzelnen Zugriffe auf ID Austria durch Nutzer* innen gespeichert und wird auf diese Weise das Tracking von Nutzer*innen ermöglicht?*

Ja, siehe dazu § 18 Abs. 1 letzter Satz E-GovG. Ein "Tracking" wird durch den Einsatz von technischen und organisatorischen Maßnahmen verhindert. So werden beispielsweise nur die vom E-ID-System übermittelten Attribute ohne die konkreten Attributwerte protokolliert, und die Protokolldaten werden nach einem Jahr gelöscht. Bei der Protokollierung wird mit dem bPK zur eindeutigen Identifikation gearbeitet, nicht mit Vor- und Nachnamen.

Antwort zu Punkt 18 der Anfrage:

18. *Laut Anfragebeantwortung 7961/AB gab es eine Datenschutzfolgeabschätzung zur Einführung von ID Austria.*
    a. *Ist diese Datenschutzfolgeabschätzung öffentlich einsehbar?*
        i. *Falls ja, wo ist diese zu finden? Bitte auch um Beifügung der Abschätzung an die Beantwortung dieser Anfrage?*
        ii. *Falls nein, warum nicht?*
        iii. *Falls nein, wird sie noch veröffentlicht oder dem Parlament vorgelegt? Und wenn ja, wann?*
    b. *Zu welchen Erkenntnissen ist diese Datenschutzfolgeabschätzung gelangt?*
    c. *Wieso wurde gerade das Unternehmen Research Institute AG & Co KG mit der Datenschutzfolgeabschätzung beauftragt?*

Eine Veröffentlichung des Berichts zur Datenschutz-Folgenabschätzung (DSFA) ist vor Aufnahme des Vollbetriebs in Aussicht genommen.

Neben einer umfangreichen Darstellung des Sachverhalts erfolgt im DSFA-Bericht die Prüfung der Zulässigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge insbesondere hinsichtlich Rechtsgrundlagen, Einhaltung datenschutzrechtlicher Grundsätze gemäß DSGVO wie Zweckbindung, Datenminimierung und Speicherbegrenzung sowie Berücksichtigung der Betroffenenrechte. Weitere Schwerpunkte in diesem Abschnitt bilden die datenschutzrechtliche Rollenverteilung sowie die datenschutzrechtlichen Anforderungen an die Protokollierung. Ein weiterer wichtiger Kernbestandteil des DSFA-Berichts ist die Risikobeurteilung. Dieser Abschnitt befasst sich mit den Maßnahmen, Garantien und Verfahren, durch die allfällige Risken der geplanten Verarbeitung eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen der DSGVO nachgewiesen werden.

Im Ergebnis zeigt der DSFA-Bericht, dass die identifizierten bzw. verbleibenden Risiken aufgrund der gesetzten Maßnahmen des Verantwortlichen für die Betroffenen in ihrer Eintrittswahrscheinlichkeit und Schwere nicht als hoch einzustufen sind. Aus derzeitiger Sicht besteht somit auch keine Notwendigkeit zur Konsultation der Aufsichtsbehörde nach Artikel 36 DSGVO.

Beim Unternehmen Research Institute AG & Co KG (RI) handelt es sich um eine etablierte und innerhalb der Community anerkannte Organisation, die insbesondere im Bereich des Datenschutzes und Datensicherheit über große Expertise verfügt. Laut eigenen Angaben steht das RI im regelmäßigen fachlichen Austausch mit Organisationen wie noyb.eu, epicenter.works sowie Internet Service Providers Austria und ist Mitglied im Wiener Zentrum für Rechtsinformatik. Mit der Beauftragung des RI ist eine genaue, wissenschaftlich wertvolle und zugleich objektive Beurteilung der Systeme und Sicherheitsmaßnahmen gewährleistet.

Antwort zu Punkt 19 der Anfrage:

19. *Ist geplant, für die in Entwicklung befindliche Ausweisplattform, welche gerade durch die Staatsdruckerei entwickelt wird, ebenfalls eine Datenschutzfolgeabschätzung vorzunehmen?*
    a. *Falls ja, wird diese dann veröffentlicht?*
    b. *Falls nein, wieso nicht?*

Für die Ausweisplattform wird eine gesonderte Datenschutzfolgeabschätzung erstellt, deren Veröffentlichung in Aussicht genommen ist.

Antwort zu Punkt 21 der Anfrage:

21. Gab es in der Vergangenheit Zugriffe von Strafverfolgungsbehörden auf die Daten der A-Trust im Rahmen der Handysignatur?

Hinsichtlich der bei der A-Trust verarbeiteten Daten liegen meinem Ressort keine Informationen vor, da die A-Trust datenschutzrechtlich für diese Daten verantwortlich ist.

Antwort zu Punkt 24 der Anfrage:

24. Die Handysignatur steht Menschen zur Verfügung, die 14 Jahre oder älter sind. Wird dies bei der ID Austria auch der Fall sein?
   a. Falls ja, wie wird der besondere Schutz von Minderjährigen und deren Daten im Rahmen der Verwendung der ID Austria gewährleistet?

Ja, vergleiche dazu § 4a Abs. 1 E-GovG. Der besondere Schutz von Minderjährigen wurde bei der Erstellung des DSFA-Berichts in der Risikobeurteilung berücksichtigt. Die Maßnahmen, Garantien und Verfahren, durch die auch das Risiko der Verarbeitung von personenbezogenen Daten Minderjähriger eingedämmt und die Einhaltung der Bestimmungen der DSGVO nachgewiesen werden, werden nach Veröffentlichung im Detail dem DSFA-Bericht zu entnehmen sein.

Antwort zu Punkt 25 der Anfrage:

25. Welche (technischen) Vorrausetzungen braucht ein Endgerät, um ID Austria nutzen zu können? Wird es möglich sein, die ID Austria ohne Smartphone zu nutzen?
   a. Falls ja, wie wird dies konkret ausgestaltet sein?
   b. Falls nein, wird es für jene Menschen, die bisher die Handysignatur ohne Smartphone nutzten, ein alternatives Angebot geben?

Smartphones mit iOS ab iPhone 6s (2015) müssen über Secure Enclave verfügen, Android-Smartphones ab Android 8 über Fingerprint oder dedizierte Gesichtserkennung, alternative Geräte benötigen ein FIDO-Token.

Antwort zu Punkt 26 der Anfrage:

26. Wird es die Möglichkeit geben, ID Austria auch mit einem alternativen App Store (Huawei, F-Droid, etc.) oder auf einem Smartphone ohne Google oder Apple Betriebssystem zu nutzen?
   a. Falls nein, wodurch ist diese Einschränkung sachlich gerechtfertigt?

Aktuell ist dies nicht geplant, da vorgesehen ist, jene Betriebssysteme zu unterstützen, die einen signifikanten Marktanteil abdecken.

Antwort zu Punkt 27 der Anfrage:

27. Auf der Website der ID Austria (https://www.oesterreich.gv.at/id-austria) heißt es, dass man sich mit dem digitalen Weg zum Amt bis zu 40 % der Antragsgebühren sparen könne. Wie begegnen Sie dieser groben Diskriminierung von jenen Menschen, die weniger digital affin sind oder kein Smartphone mit Datentarif und biometrischer Authentifizierung leisten können und denen es somit nicht möglich ist, das digitale Amt zu nutzen?

Die Abwicklung von Amtswegen auf elektronischem Weg ist ein Angebot der öffentlichen Verwaltung, das die Anforderungen der Barrierefreiheit berücksichtigt und auch die damit verbundenen Einsparungspotentiale an die Antragsteller weitergibt. Personen, denen eine Smartphonenutzung nicht möglich ist, können dies über alternative Methoden (FIDO-Token) tun.

Antwort zu Punkt 28 der Anfrage:

28. Wird es ein Angebot für die ID Austria für jene Menschen ohne Smartphone mit Datentarif und biometrischer Authentifizierung geben?
   a. Falls ja, wann und auf welcher Plattform wird dieses angeboten werden?
   b. Falls nein, begegnet das Ministerium der Benachteiligung dieser Bevölkerungsschichten beim Zugang zu staatlichen Leistungen und etwaiger Mehrkosten bei Behördenwegen?

Ja. Um allen Handy-Signatur-Nutzerinnen und -Nutzern und allen zukünftigen ID Austria-Nutzern den digitalen Zugang zu ermöglichen, werden Alternativlösungen zur Authentifizierung mittels Smartphone angeboten werden, so etwa über einen FIDO-Token als zweiten Authentifizierungsfaktor. Auch gültige Signaturkarten werden als zweiter Faktor be-

rücksichtigt werden. Im Self-Service-Bereich von ID Austria wird es möglich sein, diese Alternativlösungen hinzuzufügen.

Antwort zu Punkt 29 der Anfrage:

29. Wurde bei der Konzipierung und Programmierung von ID Austria darauf geachtet, dass die Anwendung auch für weniger digitalaffine Personen nutzbar ist?

- *a. Welche Personengruppen haben ID Austria in der Pilotphase getestet? Waren darunter auch weniger digitalaffine Personen?*
- *b. Welche Anstrengungen wurden unternommen, um die ID Austria auch für Menschen mit Behinderung nutzbar zu machen?*
- *c. Was wurde/wird getan, um ID Austria für möglichst viele Bevölkerungsgruppen, auch weniger digitalaffinen, nutzbar zu machen?*
- *d. Wie benutzer*innenfreundlich wurde ID Austria gestaltet? Wird es eine reduzierte, "easy-use" Version der Anwendung geben, um die Nutzung auch wenig digitalaffinen Personen zu ermöglichen?*
- *e. Wird es Einschulungsangebote oder ähnliches geben, um auch weniger digitalaffine Personengruppen zu erreichen?*
- *f. Wird es zur Einführung von ID Austria allgemeine Werbe- und/oder Informationskampagnen geben?*

Ja, die Pilotphase steht allen Benutzerinnen und Benutzern offen; eine Einschränkung auf bestimmte Personengruppen ist nicht erfolgt.

Bei der Konzeption und Entwicklung von oesterreich.gv.at und der App Digitales Amt wurden Anforderungen gemäß WCAG 2.1 AA umgesetzt. An der kontinuierlichen Verbesserung der Barrierefreiheit wird gearbeitet. Eine Expertenanalyse der App Digitales Amt und der Benutzeroberflächen wurde durchgeführt. Erkenntnisse und Optimierungspotenziale hinsichtlich der Barrierefreiheit sind erfasst und in Entwicklung.

Ein Austausch mit Stakeholdergruppen hat stattgefunden und wird auch weiter gepflegt. Es wird eine Serviceline bereitgestellt, die bei Nutzungsherausforderungen zur Verfügung steht. Weiters wurden Schritt-für-Schritt Anleitungen erarbeitet und zur Verfügung gestellt.

Es wurden User Experience Tests durchgeführt, um die Nutzerfreundlichkeit der Prozesse zu evaluieren. Eine Version mit reduziertem Funktionsumfang ist nicht geplant. Nutzerinnen und Nutzer sollen selbst entscheiden können, welchen Teil des Angebots sie nutzen

möchten. Die Nutzung der ID Austria wurde möglichst einfach und bedienerfreundlich gestaltet. Die Informationsseiten auf www.id-austria.gv.at bieten für weniger digitalaffine Personengruppen Unterstützung bei den ersten Schritten in der Bedienung und werden aus der Erfahrung des Betriebes laufend weiter ausgebaut.

Informationsmaßnahmen im Zusammenhang mit der Aufnahme des Vollbetriebs der ID Austria sind geplant, um Bürgerinnen und Bürger, aber auch Unternehmen auf den Umstieg von der Handysignatur und die Möglichkeiten der Nutzung der ID Austria aufmerksam zu machen.

Antwort zu Punkt 30 der Anfrage:

30. Auf EU-Ebene wird im Moment eine Reform der e IOAS Verordnung verhandelt, mit der eine "Neugestaltung des europäischen Rechtsrahmens für elektronische Identitätssysteme (e/D)" (vgl. https://epicenter.works/document/ 3895) umgesetzt werden soll.
   a. Orientiert sich ID Austria am derzeitig bestehenden europäischen Rechtsrahmen für elektronische Identitätssysteme?
   b. Mit der Neugestaltung des genannten EU-Rechtsrahmens, besteht die Gefahr, dass ID Austria dann nicht mehr den Vorgaben und Normen der EU Verordnung entspricht?
      i. Falls ja, wie wird dieser Widerspruch aufgelöst?

Ende September 2021 begann auf EU-Expertenebene der "peer review"-Prozess zur ID Austria Österreich. Spezialistinnen und Spezialisten aus zahlreichen EU-Mitgliedstaaten prüften dabei die derzeit im Pilotbetrieb befindliche ID Austria. Das Ergebnis liegt seit 21. Februar 2022 vor; darin bescheinigt das eIDAS-Kooperationsnetz, dass die ID Austria den höchsten Sicherheitsanforderungen auf EU-Ebene entspricht. Die positive Stellungnahme des eIDAS-Kooperationsnetzes war die Voraussetzung dafür, dass die förmliche Notifizierung des österreichischen elektronischen Identitätsnachweises am 28. Februar 2022 vorgenommen werden konnte. Daran schließt eine Kundmachung durch die Europäische Kommission im Amtsblatt der Europäischen Union an, gefolgt von einer maximal zwölfmonatigen Übergangsfrist für die Mitgliedstaaten. Es ist damit sichergestellt, dass Nutzerinnen und Nutzer der ID Austria spätestens im Laufe des Jahres 2023 ihre ID Austria auch für Anwendungen in ganz Europa nutzen können.

Österreich beteiligt sich aktiv in den Diskussionen über den EU-Rechtsrahmen und versucht, die Architekturkonzepte von ID-Austria als im EU-Rahmen integrierbar zu gestalten. Konkrete Änderungsnotwendigkeiten sind gegenwärtig nicht abzusehen.

Wien, am 23. Mai 2022

Univ.-Prof. Dr. Martin Kocher

Elektronisch gefertigt

Unterzeichner	Bundesministerium für Digitalisierung und Wirtschaftsstandort
Datum/Zeit	2022-05-23T17:22:42+02:00
Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Serien-Nr.	1237897311
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/. Die Bildmarke und Hinweise zur Verifikation eines Papierausdrucks sind auf https://www.bmdw.gv.at/amtssignatur oder http://www.help.gv.at/ veröffentlicht.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-05-23T17:25:46+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	