BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.250/0002-DSR/2017
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundeskanzleramt

Per E-Mail:
i11@bka.gv.at

Betrifft: Bundesgesetz, mit dem das E-Government-Gesetz geändert wird
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **234. Sitzung am 22. Mai 2017 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Laut den Erläuterungen zum Entwurf ergibt sich der Anpassungsbedarf im E-Government-Gesetz (E-GovG) einerseits aufgrund der Notwendigkeit der Umsetzung unionsrechtlicher Vorgaben. Die eIDAS-Verordnung (eIDAS-VO) harmonisiert nicht die bereits in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme und zugehörige Infrastrukturen, sondern schafft den Rechtsrahmen zur gegenseitigen Anerkennung der verschiedenen elektronischen Identifizierungsmittel unter bestimmten normierten Voraussetzungen. **Mit dem vorliegenden Entwurf sollen die rechtlichen Rahmenbedingungen geschaffen werden, um notifizierte elektronische Identifizierungsmittel anderer EU-Mitgliedstaaten für österreichische Online-Services gleichwertig verwenden zu können, sofern die notwendigen Voraussetzungen vorliegen.**

Andererseits wird im Sinne eines sicheren, modernen, digitalen Identitätsmanagements die Bürgerkarte hin zu einem umfassenden

elektronischen Identitätsnachweis (E-ID) weiterentwickelt. Dabei wird nicht nur ein Augenmerk auf einen sicheren, behördlichen Registrierungsprozess gelegt, sondern es werden auch die Nutzungsmöglichkeiten eines elektronischen Identitätsnachweises maßgeblich erweitert. **Im Vergleich zur Bürgerkarte soll es mit dem E-ID künftig auch möglich sein, an Dritte den Nachweis von Daten aus Registern von Auftraggebern des öffentlichen Bereichs (etwa Personenstands-, Melde- oder Staatsbürgerschaftsdaten) zu erbringen.**

Wesentlicher und integraler Bestandteil des neuen E-ID-Systems ist der hoheitliche Registrierungsprozess. Die Vornahme der Registrierung bei inländischen Behörden, die üblicherweise mit der Überprüfung von Identitätsdokumenten betraut sind, trägt maßgeblich zur Feststellung der eindeutigen Identität und damit zu einem sicheren Registrierungsprozess bei.

Die bewährte Funktion der österreichischen Bürgerkarte (nunmehr: E-ID), insbesondere in ihrer Ausprägung als Handy-Signatur, bleibt somit laut den Erläuterungen grundsätzlich bestehen und erfährt im Hinblick auf die künftige rechtliche Anerkennung in den anderen EU-Mitgliedstaaten eine deutliche Ausweitung ihrer Einsatzmöglichkeiten. Durch eine gegenseitige Anerkennung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten zumindest die Authentifizierung für öffentliche Dienste ermöglichen, soll die grenzüberschreitende Erbringung von Dienstleistungen im Binnenmarkt deutlich erleichtert und der „digitale Binnenmarkt“ insgesamt gestärkt werden. Im Hinblick auf die Interoperabilität der österreichischen Lösung, aber auch um die Voraussetzungen für die Anerkennung elektronischer Identifizierungsmittel anderer Mitgliedstaaten in Österreich zu schaffen, sind diverse legistische Anpassungen notwendig. Weiters wird mit dieser Novelle der technischen Weiterentwicklung Rechnung getragen und an einigen Stellen im Gesetz werden Klarstellungen vorgenommen.

Die Änderungen im E-GovG sollen laut den Erläuterungen insgesamt ein einheitliches Rahmenwerk für das elektronische Identitätsmanagement bieten und den ordnungspolitischen Rahmen für den Umgang mit elektronischen Identitätsnachweisen sicherstellen.

Die Hauptgesichtspunkte des Entwurfs sind:

- Weiterentwicklung der **„Bürgerkarte“** zu einem **„Elektronischem Identitätsnachweis (E-ID)“**
- Zukünftig sollen **Applikationen** – sei es aus dem hoheitlichen oder dem privaten Bereich – bereichsspezifische Personenkennzeichen nicht mehr selbst berechnen dürfen. Dieser Vorgang soll an einer vertrauenswürdigen, zentralen

Stelle (Stammzahlenregisterbehörde bzw. bei einem ihrer Dienstleister) vorgenommen werden. Dies ermöglicht es auch nicht österreichischen Applikationen, den österreichischen E-ID ohne zusätzlichen Aufwand zu integrieren.

- Bei jeder **Verwendung des E-ID** wird immer eine Personenbindung erstellt und signiert oder besiegelt. Damit wird auch gewährleistet, dass andere Mitgliedstaaten diese aus Österreich stammenden Personenidentifizierungsdaten sofort verifizieren können.
- Der **Registrierungsprozess eines E-ID** wird in Bezug auf die Sicherstellung der eindeutigen Identifizierung des E-ID-Werbers auf ein noch höheres Niveau gehoben. Die Identifizierung des E-ID-Werbers soll nunmehr ausschließlich bei Passbehörden, bei nach § 16 Abs. 3 Passgesetz 1992, BGBl. Nr. 839/1992, ermächtigten Gemeinden, Landespolizeidirektionen oder anderen geeigneten Behörden möglich sein. Im Zuge der Beantragung eines Reisedokuments wird die Registrierung eines E-ID nun von Amts wegen durchgeführt. Weiters wird im Registrierungsprozess eines E-ID die Möglichkeit geschaffen, die vorgelegten Ausweisdaten (wie zB. Reisepassnummer) in den entsprechenden Registern abzufragen und gegenüber den von Sicherheitsbehörden geführten Fahndungsevidenzen abzugleichen, um damit das Risiko mindern zu können, dass die Identität der Personen nicht mit der beanspruchten Identität übereinstimmt.
- Neben den **Kernidentitätsdaten** (Vorname, Familienname, Geburtsdatum) sollen in Zukunft für Personen **auch weitere Merkmale** (zB Staatsbürgerschaft) in gesicherter Form einer Datenanwendung im öffentlichen Bereich zur Verfügung gestellt werden können. Bei der Verwendung des E-ID im privaten Bereich wird jedenfalls ein bPK zum E-ID-Inhaber zur Verfügung gestellt. Vorname, Familienname, Geburtsdatum bzw. weitere Merkmale können in die Personenbindung optional eingefügt werden, wenn der Betroffene dem zustimmt.
- **Elektronische Identifizierungsmittel anderer Mitgliedstaaten der EU**, die die Anforderungen nach Art. 6 Abs. 1 eIDAS-VO erfüllen, sollen in Österreich spätestens sechs Monate nach deren Notifizierung gemäß Art. 9 eIDAS-VO wie ein E-ID für Zwecke der eindeutigen Identifikation verwendet werden können.
- Für **Personen**, die ein **notifiziertes elektronisches Identifizierungsmittel** eines anderen Mitgliedstaates verwenden, wird – sofern ein solcher nicht bereits besteht – ein Eintrag im Ergänzungsregister und eine Personenbindung wie bei Verwendung des E-ID erstellt. Der allfällige Eintrag im Ergänzungsregister erfolgt

auf Basis der vom notifizierten elektronischen Identifizierungsmittel des anderen Mitgliedstaates übermittelten Daten.

- Es werden **Haftungsbestimmungen** im Einklang mit den Vorgaben der eIDAS-VO eingeführt.
- Weiters soll mit dieser Novelle der technischen Weiterentwicklung der **elektronischen Einzelvertretungsbefugnisse** Rechnung getragen werden. Die Einzelvertretungsbefugnis kann von der Stammzahlenregisterbehörde in die Personenbindung eingefügt und somit der Applikation zur Verfügung gestellt werden. Dabei darf die Stammzahlenregisterbehörde auch auf Angaben zu Vertretungsverhältnissen in Datenanwendungen anderer Auftraggeber des öffentlichen Bereichs (zB das Unternehmensserviceportal) zurückgreifen.

2) Datenschutzrechtlich relevante Bestimmungen

Artikel 1 (Änderung des E-Government-Gesetzes)

Datenschutzrechtliche Vorbemerkungen

1. Vorweg erscheint nicht nachvollziehbar, welche Bestimmungen des Entwurfes sich auf den in den Erläuterungen angeführten **Kompetenztatbestand des § 2 DSG 2000** stützen. Diesbezüglich sollten entsprechende Ausführungen in den Erläuterungen getätigt werden.

In den Erläuterungen wird zudem ausgeführt, dass sich der Anpassungsbedarf im E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004, auch aufgrund der **Notwendigkeit der Umsetzung unionsrechtlicher Vorgaben** ergibt. Es sollte ausführlicher erläutert werden, welche Bestimmungen im vorliegenden Entwurf davon umfasst sind.

Mehrfach wird im Entwurf (zB in den §§ 4, 5, 6 Abs. 5 und 14 Abs. 3) auf die „**Personenbindung“** Bezug genommen. Es sollte in den **Erläuterungen verständlicher dargestellt werden**, zu welchem Zweck die Personenbindung benötigt wird und wie diese konkret vorgenommen wird.

Auch sollte erläutert werden, ob die mehrfach im Entwurf (zB in den §§ 4, 5 und 12) verwendete „**Zustimmung“** der **datenschutzrechtlichen Zustimmung** gemäß § 4 Z 14 DSG 2000 entspricht und daher die datenschutzrechtlichen Anforderungen an eine gültige Zustimmung erfüllt sein müssen.

2. Soweit der Entwurf **neue Datenanwendungen** enthält, wird darauf hingewiesen, dass den Auftraggeber einer Datenanwendung nach den Vorgaben der §§ 17 ff DSG 2000 eine Meldepflicht an das Datenverarbeitungsregister trifft.

Der Datenschutzrat regt daher an, diesbezüglich rechtzeitig mit der unabhängigen **Datenschutzbehörde** in Kontakt zu treten.

Aufklärungsbedürftig erscheint, ob bzw. wie sich die vorgeschlagenen Änderungen des E-GovG auf bereits bestehende und **in Materiengesetzen geregelte Datenanwendungen** auswirken, dies etwa im Hinblick auf die **Einführung des Elektronischen Identitätsnachweises (E-ID)** sowie die in Gesetzen vorgesehene **Verwendung der Bürgerkarte und des bereichsspezifischen Personenkennzeichens**. Es sollte näher erläutert werden, ob sich durch diese Änderungen ein **weiterer Anpassungsbedarf** bzw. eine **Änderung bestehender Datenanwendungen** ergibt, die allenfalls auch eine **Meldepflicht nach §§ 17 ff DSG 2000 (Änderungsmeldung)** auslösen kann.

3. Grundsätzlich wird zudem darauf hingewiesen, dass ab dem 25. Mai 2018 die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG **(Datenschutz-Grundverordnung – DSGVO)** zur Anwendung kommt und in der Europäischen Union unmittelbar gilt. Die derzeit geltende Form der **Meldepflicht an das Datenverarbeitungsregister** (§§ 17 ff DSG 2000) wird aufgrund der Anwendung der DSGVO ab dem 25. Mai 2018 entfallen.

Damit wird auch eine Anpassung an die Terminologie der DSGVO im E-Government-Gesetz notwendig sein.

Anstelle des Meldeverfahrens sieht die DSGVO unter bestimmten Voraussetzungen in Art. 35 die **Einführung einer Datenschutz-Folgenabschätzung** durch den datenschutzrechtlich Verantwortlichen (derzeit: „Auftraggeber“) vor. Eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DSGVO ist insbesondere in den Fällen des Abs. 3 erforderlich.

Art 35 Abs. 10 DSGVO sieht unter den angeführten Voraussetzungen eine **Ausnahme von der Datenschutz-Folgenabschätzung** durch Verantwortliche für Verarbeitungen vor, die auf einer **Rechtsgrundlage im Recht des Mitgliedstaates**, dem der Verantwortliche unterliegt, beruhen und falls diese Rechtsvorschriften den **konkreten Verarbeitungsvorgang** oder die **konkreten Verarbeitungsvorgänge** regeln und bereits **im Rahmen der allgemeinen Folgenabschätzung** im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine **Datenschutz-Folgenabschätzung erfolgte**.

Der Erwägungsgrund 84 der DSGVO weist zur Datenschutz-Folgenabschätzung ua. darauf hin, dass der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die **Ursache, Art, Besonderheit und**

Schwere dieses Risikos evaluiert werden, verantwortlich sein soll. Die **Ergebnisse der Abschätzung** sollten berücksichtigt werden, wenn darüber entschieden wird, **welche geeigneten Maßnahmen ergriffen werden müssen**, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht.

Geht aus einer Datenschutz-Folgenabschätzung hervor, dass **Verarbeitungsvorgänge ein hohes Risiko** bergen, das der Verantwortliche **nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann**, muss nach dem Regelungsregime der DSGVO die **Aufsichtsbehörde (Datenschutzbehörde) vor Beginn der Verarbeitung konsultiert werden**.

In diesem Sinne wird – im Falle, dass eine Datenschutz-Folgenabschätzung **nach den Vorgaben des Art. 35 DSGVO erforderlich ist** – angeregt, bei dem vorliegenden Vorhaben zu prüfen, **ob im Rahmen der allgemeinen Folgenabschätzung die Datenschutz-Folgenabschätzung (zum Inhalt siehe insbesondere Art. 35 Abs. 7 DSGVO) bereits vorweggenommen und die konkrete Datenanwendung entsprechend gesetzlich angeordnet werden kann.**

In den **Erläuterungen** sollte diesfalls die **Durchführung der Datenschutz-Folgenabschätzung** gemäß Art. 35 Abs. 7 DSGVO ausführlich dargelegt und wie in der DSGVO verlangt beschrieben werden. Im Gesetz selbst könnte – nach Ansicht des Bundeskanzleramtes-Verfassungsdienst – folgende Anordnung getroffen werden:

„(x) Die aufgrund dieses Abschnittes vorzunehmende(n) Datenverarbeitung(en) erfüllt(en) die Voraussetzungen des Art. 35 Abs. 10 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, für einen Entfall der Datenschutz-Folgenabschätzung.“

Ansonsten sollte die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO vom jeweiligen Verantwortlichen bis spätestens 24. Mai 2018 vorgenommen werden.

Der Datenschutzrat hat durch den informierten Vertreter zur Kenntnis genommen, dass eine diesbezügliche gesetzliche Regelung geprüft wird.

Zum Gesetzesentwurf

Zu Z 11 (§ 4):

Es sollte bereits aus dem Gesetzestext hervorgehen, welche **„weiteren Merkmale“** in die Personenbindung eingefügt werden können, da sonst nicht vorhersehbar ist, **welche Daten** verwendet werden können. Fraglich erscheint zudem, ob allenfalls auch **sensible Daten** (§ 4 Z 2 DSG 2000) – etwa das **Religionsbekenntnis** – als **„weiteres Merkmal**“ verwendet werden können.

Unklar erscheint, welche konkreten **Register von Auftraggebern des öffentlichen Rechts** gemäß § 4 Abs. 5 für die Stammzahlenregisterbehörde zugänglich sein sollen. Dies sollte ausführlich dargelegt werden.

Zu § 4 Abs. 8 wird angemerkt, dass im Gesetzestext konkreter geregelt werden sollte, **welche „näheren“ Regelungen** zu den Abs. 1 bis 7 im Rahmen einer **Verordnung** getroffen werden können.

Zu Z 12 (§§ 4a und 4b):

1. Nachdem die **Registrierung der Funktion E-ID** gemäß § 4a Abs. 1 für Staatsbürger im Rahmen der **Beantragung eines Reisedokumentes** nach dem Passgesetz 1992, BGBl. Nr. 839/1992, **von Amts wegen vorzunehmen ist**, sollte iSd in § 1 Abs. 2 DSG 2000 verankerten **Verhältnismäßigkeitsgrundsatzes** zumindest in den Erläuterungen dargelegt werden, weshalb diese **Registrierung von Amts wegen** bei der Beantragung eines **Reisedokumentes** zur Zweckerreichung unbedingt **erforderlich** ist und das **gelindeste Mittel** darstellt.

Die **Veröffentlichung** von **anderen geeigneten Behörden**, die die Registrierung des E-ID vornehmen, sollte nicht im Internet, sondern auch in Form einer **Verordnung** vorgenommen werden, da diese **Behörden** im Zuge der Registrierung auch **personenbezogene Daten des Staatsbürgers** verwenden.

Hinsichtlich der in § 4a Abs. 6 geregelten **Festlegung der Vorgangsweise gemäß Abs. 1 bis 5 durch Verordnung** wird auf die Anmerkungen zu § 4 Abs. 8 verwiesen.

Der Datenschutzrat hat zur Kenntnis genommen, dass die vorgesehene „Opt-Out-Lösung“ in den Erläuterungen ausgeführt wird und klargestellt wird, ob mit der Verordnung in die Unabhängigkeit der Datenschutzbehörde eingegriffen werden könnte.

2. In den Erläuterungen wird bei den **Hauptgesichtspunkten** sowie zu § 4a Abs. 4 darauf Bezug genommen, dass im **Registrierungsprozess eines E-ID** die Möglichkeit geschaffen wird, die vorgelegten Ausweisdaten (zB Reisepassnummer) in den entsprechenden Registern abzufragen und **gegenüber den von Sicherheits-**

behörden geführten Fahndungsevidenzen abzugleichen. § 4a Abs. 4 ist nach Ansicht des Datenschutzrates für einen derartigen Datenabgleich und Eingriff in das Grundrecht auf Datenschutz jedoch **zu weit und nicht ausreichend konkret ausgestaltet**, da aus dieser Bestimmung insbesondere nicht hervorgeht, **welche konkreten Datenanwendungen** davon umfasst sind bzw. ob die **Abfrage zur Zweckerreichung überhaupt erforderlich und verhältnismäßig** ist. Schon aus diesen Gründen **entspricht § 4a Abs. 4 nicht den Vorgaben des § 1 Abs. 2 DSG 2000** für einen Eingriff durch eine **„staatliche Behörde"** in das Grundrecht auf Datenschutz.

Weiters ergibt sich aus dem Gesetzeswortlaut **nur eine Abfrage dieser Daten, nicht jedoch ein Datenabgleich** in der Form einer Einmeldung von geänderten Daten.

Fraglich ist, in welchem Verhältnis die Ermächtigung nach § 4a Abs. 4 zur **Vorgabe nach § 4b** steht, wonach die Verwendung von den in dieser Bestimmung genannten Daten **zu anderen Zwecken als der Verwaltung der E-ID nur aufgrund besonderer gesetzlicher Anordnung zulässig ist.**

Zu § 4b wird angemerkt, dass fraglich ist, **wozu die Telefonnummer eines Mobiltelefons und die E-Mail-Adresse überhaupt benötigt werden** und wie bei einer **Änderung dieser Daten** zu verfahren ist bzw. ob der Betroffene auch eine **Verpflichtung** hat, eine derartige Änderung zu melden.

Zu Z 13 (§ 5):

Völlig unklar ist, welche **Datenanwendungen anderer Auftraggeber des öffentlichen Bereichs** in § 5 Abs. 1 in Betracht kommen.

Zu Z 27 (§ 14 Abs. 3):

Im Hinblick auf die **für das Stammzahlenregister zugänglichen Register** von Auftraggebern des öffentlichen Bereichs wird auf die Anmerkungen zu Z 11 (§ 4) verwiesen.

Zu Z 28 (§ 14a):

Hinsichtlich der Einfügung **weiterer Merkmale aus für die Stammzahlenregisterbehörde zugänglichen Registern** von Auftraggebern des öffentlichen Bereichs wird auf die Anmerkungen zu Z 11 (§ 4) verwiesen.

Zu Z 31 (§ 18):

Die in § 18 Abs. 1 geregelte **Zurverfügungstellung von personenbezogenen Daten an Dritte** sollte ausführlicher erläutert werden. Insbesondere sollte dargelegt werden, welche **gesetzlichen Ermächtigungen** nach § 18 Abs. 1 Z 3 in Frage kommen.

Unklar ist nach dem Gesetzestext auch, welchen **„Dritten“** gemäß § 18 Abs. 2 die **Nutzung des E-ID-Systems** eröffnet werden kann. Diesbezüglich müssten – über den Grundsatz von Treu und Glauben hinaus – **weitere Datensicherheitsmaßnahmen gemäß § 14 DSG 2000** (zB Zutritts- bzw. Zugangsbeschränkungen und Dokumentationspflichten) im Gesetz festgelegt werden. In diesem Sinne erscheint auch nicht nachvollziehbar, weshalb gemäß § 18 Abs. 3 die **Protokollierung deaktiviert** werden kann. Dies sollte zumindest näher erläutert werden.

Zu Z 34 (§ 25 Abs. 2 und 3):

Es wird darauf hingewiesen, dass für **Pilotbetriebe**, in denen (personenbezogene) Echtdaten verwendet werden, **keine Ausnahmen im DSG 2000** bestehen. Dies betrifft insbesondere auch die **Meldepflicht an das DVR** nach den §§ 17 ff DSG 2000 und das Ergreifen von § 14 DSG 2000 entsprechenden **Datensicherheitsmaßnahmen.** Mit der DSGVO kommen die darin vorgesehenen Maßnahmen zur Datensicherheit zur Anwendung.

Abschließende Feststellung des Datenschutzrates

Der Schutz digitaler Identitäten ist zentrale Voraussetzung für das Funktionieren eines digitalen europäischen Binnenmarktes. Die Einrichtung eines elektronischen Identitätsnachweises (E-ID) nach dem E-Government-Gesetz stellt daher ebenso eine Notwendigkeit dar wie die Prüfung neuer IT-Technologien.

So ist aus Sicht des Datenschutzrates auch der zukünftige Einsatz von „Block-chain“ zum Schutz der „digitalen (virtuellen) Identität“ zu prüfen.

23. Mai 2017
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt