Bundesministerium
Digitalisierung und Wirtschaftsstandort
I/A/2 Internationale Beziehungen und
Legistik
Stubenring 1
1010 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
2020-0.501.921	BAK/KS-GSt/DZ/BE	Daniela Zimmer	DW 12722	DW 12693	09.10.2020

Entwurf eines Bundesgesetzes, mit dem das E-Government-Gesetz und das PassG geändert werden

Sehr geehrte Damen und Herren!

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfes und nimmt dazu wie folgt Stellung:

Ziel des Entwurfes:
Das bisherige Konzept der Bürgerkarte soll zu einem elektronischen Identitätsnachweis (E-ID) weiterentwickelt werden. Die Anpassung des Rechtsrahmens dient zunächst nur der rechtlichen Absicherung des E-ID-Probebetriebs (Momentan fehlt es nämlich noch an den Voraussetzungen für den E-ID-Echtbetrieb, etwa einer sicherheitstechnisch gleichwertigen Umsetzung der Bürgerkarte über eine Handy-App). Außerdem dürfen Registerdaten privatwirtschaftlicher Anbieter über die E-ID bei Vorliegen einer Einwilligung der NutzerInnen Dritten zur Verfügung gestellt werden (die Erläuterungen verweisen zur Illustration beispielshaft auf kommunale Verkehrsverbünde, Banken, Versicherungen, Autofahrerclubs uvm). Außerdem werden Anpassungen im Passgesetz vorgenommen.

Zusammenfassende Bewertung

- **Technische Erklärungen verständlich gestalten:** Der Entwurf bezieht sich auf komplexe technische Vorgänge. Diese werden Rechtsinteressierten, die in das Projekt nicht direkt involviert sind, auch in den Erläuterungen nur rudimentär und nicht allgemein verständlich erklärt. Entsprechend moniert auch der Datenschutzrat, dass sich der Entwurf angesichts der „komplexen technischen Regelungsmaterie“ als „sehr schwer verständlich erweist und überarbeitet und umformuliert werden sollte.“ Diesem Befund schließen wir uns an.

- **Rechtsklarheit verbessern:** Nicht nur die technischen Prozessverläufe werden kursorisch und für am Projekt Unbeteiligte kaum nachvollziehbar dargestellt. Auch der Normtext wirft mit vielen unpräzisen Formulierungen zahlreiche Fragen auf. Eine sorgfältige Analyse, ob das Vorhaben in jeder Hinsicht DSGVO-konform ist und den Interessen von BürgerInnen/KonsumentInnen an möglichst hohen Sicherheitsstandards entspricht, ist vor diesem Hintergrund kaum möglich. Vor diesem Hintergrund ist aus BAK-Sicht auch das offenkundige Fehlen einer datenschutzrechtlichen Folgenabschätzung zu beanstanden.

- **Datenschutzrat einbeziehen:** Bei der Überarbeitung des Entwurfes sollte die Stellungnahme des Datenschutzrates vom 28.9.2020 als datenschutzrechtlicher Maßstab dienen (abrufbar unter https://www.bmj.gv.at/themen/datenschutz/datenschutzrat.html). Dieser ortet nicht nur erheblichen Verbesserungsbedarf bei „sehr schwer verständlichen" Formulierungen, sondern auch bei etlichen Vorgaben, die nicht dem Bestimmtheitsgebot des Art 18 B-VG entsprechen.

- **Identifikation via Handy auch ohne Biometrie:** NutzerInnen, die einer Verwendung biometrischer Merkmale zu ihrer Identifikation nicht zustimmen können (Endgeräte ohne entsprechende Funktion) oder wollen (datenschutzrechtlicher Zustimmungsbedarf), sollte eine Handy-basierte Alternative zur biometrischen Identifikation via Handy-App angeboten werden. Dies erscheint uns angesichts des höheren Nutzungsgrad von Smartphones (gegenüber PCs) notwendig. Ein Alternativservice garantiert zudem, dass die ausdrückliche Zustimmung der NutzerInnen zur Verwendung sensibler, biometrischer Daten tatsächlich in jeder Hinsicht freiwillig und ohne Zwang erfolgt.

- **Fehlende Datenschutz-Folgenabschätzung unbedingt nachholen:** Es ist eine wirkungsorientierte Folgenabschätzung gemäß Art 35 DSGVO durchzuführen bzw zu begründen, weshalb man der Meinung ist, dass eine solche nicht erforderlich ist. Soweit Technik oder (biometrische) Daten von Herstellern von Smartphones und Betriebssystemen mitgenutzt werden, muss gewährleistet sein, dass diese Daten gesichert verarbeitet und nicht rechtswidrig für andere Zwecke weitergenutzt werden. Aufgrund der US-Provenienz der meisten Anbieter ist zu klären, ob Datenübermittlungen in die USA und gegebenenfalls auf welcher zulässigen Rechtsgrundlage erfolgen (angesichts des EUGH-bedingten Wegfalls des EU-US-Abkommens „Privacy-Shield").

- **Mehr Schutz bei kommerzieller Nutzung in der Privatwirtschaft:** Eine Verwendung im privaten Bereich ist aus BAK-Sicht nur bei Vorliegen einer DSGVO-konformen Zustimmung des Inhabers einer E-ID denkbar. Dabei ist dem Nachweis der Freiwilligkeit der Einwilligung besonders Rechnung zu tragen. So muss es alternative Möglichkeiten eines Identitätsnachweises bzw Nachweises sonstiger Merkmale geben. Andere Rechtsgrundlagen der DSGVO (berechtigte Interessen, gesetzliche Anordnung) dürfen aus BAK-Sicht keinesfalls herangezogen werden. Eine entsprechende Klarstellung wäre wünschenswert.

- **Kein Ausschluss von Betroffenenrechten**: Die BAK spricht sich gegen einen Ausschluss des Widerspruchsrechts der Betroffenen aus. Vor allem die Erforderlichkeit eines vollständigen Ausschlusses eines wichtigen Datenschutzrechtes für die Betroffenen wird nicht ausreichend und nachvollziehbar begründet. Insoweit besteht der Verdacht eines überschießenden Gebrauchs der Option des Art 23 DSGVO, Ausnahmen von den Datenschutzrechten vorzusehen, und folglich einer DSGVO-widrigen Vorgangsweise.

- **Verbindliche Zuverlässigkeitskriterien für Anwender des E-ID-Systems:** Der Innenminister wird lapidar ermächtigt, Dritten die Nutzung des E-ID-Systems zu eröffnen. Es ist aus BAK-Sicht zum Schutz der KonsumentInnen bzw BürgerInnen erforderlich, festzulegen, welchem Dritten unter welchen Voraussetzungen zu welchem konkreten Zweck die Nutzung des E-ID-Systems ermöglicht werden kann. Außerdem sind präzise Kriterien für deren Zuverlässigkeitsprüfung nötig. Eine Anfrage an die Datenschutzbehörde (DSB), ob Dritte in den letzten 5 Jahren Datenschutzrecht gebrochen haben, kann dabei nicht das einzige Kriterium sein. Die DSB erhebt auch keine Daten dazu bzw führt kein Verwaltungsstrafregister. Die Verordnungsermächtigung des Innenministers, „nähere Bestimmungen über die Vorgangsweise“ festzulegen, entspricht nicht annähernd dem Bestimmtheitsgebot des Art 18 B-VG.

- **Übermittlungserlaubnis der Passbehörden DSGVO-konform nachbessern:**
  Passdaten dürften künftig auf Anfrage an Behörden und Gerichte übermittelt werden, sofern diese die Identität einer Person festzustellen haben und „dies anders nicht in der nach den Umständen gebotenen Zeit möglich ist.“ Diese Übermittlungsbefugnis ist viel zu pauschal und zu weit. Es ist datenschutzverträglicher, Betroffene zunächst um Selbstauskunft und Vorlage eines Nachweises zu ersuchen, bevor ein Datentransfer durch Passbehörden in Gang gesetzt werden darf.

Zum Entwurf im Detail:

Änderung des E Government-Gesetzes

Zu § 2 Z 10a - Abhängigkeit vom Vorhandensein biometrischer Daten und von internationalen Geräteherstellern vermeiden:

Soweit die künftige E-ID-App biometrische Merkmale zur Identitätsfeststellung heranziehen wird, die über endgeräteseitige Funktionen bereitgestellt werden, weisen wir daraufhin, dass biometrische Daten besonders schützenswert sind. Sie dürfen nur nach den strengen Bestimmungen des Artikel 9 DSGVO verwendet werden. Kritisch zu beurteilen ist dabei, dass auf Applikationen der großen Smartphone-Hersteller Google, Apple, Samsung usw zurückgegriffen wird, ohne dass die Datenschutzkonformität und Datensicherheit von deren Datenverarbeitungsprozessen zweifelsfrei sichergestellt worden ist. Die Erläuterungen gehen auf den Aspekt nicht ein oder verweisen auch nicht auf allgemein zugängliche Gutachten, die diese Aspekte bereits sorgfältig überprüft haben.

Abseits dieser Sorge sollte auch die Unsicherheit ausgeräumt werden, dass der durch die E-ID entstandene biometrische Datensatz (rechtswidrig) für andere Zwecke herangezogen werden kann.
Aufgrund der US-Provenienz der meisten Anbieter ist auch zu klären, ob im Zuge der E-ID-Nutzung Datenübermittlungen in die USA und gegebenenfalls auf welcher zulässiger Rechtsgrundlage erfolgen.

Abgesehen von der fehlenden aktuellen Folgenabschätzung besteht aus BAK-Sicht Anlass zur Sorge, dass damit auch langfristige technologische Abhängigkeiten entstünden. Sollten Geräte- oder Betriebssystemanbieter ihre Applikationen, die E-ID mit nutzt, einmal zum datenschutzrechtlichen Nachteil der NutzerInnen ändern, gäbe es keine unmittelbare Alternative. Diese Abhängigkeit ist aus Datenschutzsicht unbedingt zu vermeiden.

Angesichts dieser aus BAK-Sicht kritischen Szenarien, darf es auch keinen latenten Lenkungsdruck oder gar Zwang geben, die Handy-App samt biometrischer Funktionen zu nutzen. Da Smartphones inzwischen weitaus häufiger im Alltag benutzt werden als PCs, legt die BAK allergrößten Wert darauf, dass auch gleichwertige, leicht handhabbare, alternative Identifikationswege am Handy für diejenigen angeboten werden, die keinen biometrischen Datenabgleich wünschen.

Zu § 4 Abs. 5 – kommerzielle Verifikation „weiterer Merkmale“ präzisieren und Betroffenenrechte absichern:

Die Ermächtigung, mit Einwilligung des E-ID-Inhabers weitere Merkmale in die Personenbindung aufzunehmen, ist viel zu vage formuliert. An welche „für die Stammzahlenbehörde zugänglichen Register des öffentlichen und privaten Bereiches“ ist dabei konkret gedacht? Was bedeutet die Einschränkung „nach Maßgabe der technischen Möglichkeiten“? Welche weiteren Merkmale von Verantwortlichen des öffentlichen oder privaten Bereichs können konkret eingefügt werden?

Durch einen Verweis auf Art 4 Z 11 DSGVO ist außerdem unbedingt abzusichern, dass mit Einwilligung des E-ID-Inhabers eine datenschutzrechtliche Einwilligung nach der DSGVO gemeint ist. Explizit anzuführen ist, dass die Einbindung weiterer Merkmale ausnahmslos auf eine Einwilligung des Betroffenen (und nicht etwa auf berechtigte Interessen Dritter oder Ermächtigungsnormen in einzelnen Materiengesetzen) gestützt werden darf.

Zu § 4a Abs. 3 und 4 – Angemessenheit der Speicherdauer begründen:

Um die Angemessenheit einer Speicherdauer der Daten von E-ID-Werbern von 30 Tagen beurteilen zu können, sollte der verhältnismäßig lange Zeitraum für eine automatisierte Registrierung in den Erläuterungen näher begründet werden. Auf den Grundsatz der Speicherbegrenzung (Art 5 DSGVO) wird in diesem Zusammenhang hingewiesen.

Zu § 4b Abs 2 und 3 – kein Ausschluss des Widerspruchsrechtes; Konkretisierung der Datenarten:

Der generelle Ausschluss des Widerspruchsrechtes der betroffenen Person wird nicht nachvollziehbar begründet. Die BAK weist auf die Vorgaben des Art 23 Abs 2 DSGVO hin. Die Option, Betroffenenrechte einzuschränken, ist an strenge Kautelen geknüpft, die im vorliegenden Entwurf nicht erfüllt sein dürften. Zum Schutz der NutzerInnen und um einer EU-Rechtswidrigkeit vorzubeugen, sollte die Bestimmung ersatzlos gestrichen werden.

Nach § 4b Abs 3 dürfen die Registrierungsbehörden „Daten zu den vorgelegten Urkunden und Nachweisen" verarbeiten. Welche personenbezogenen Daten verarbeitet werden dürfen, erhellt sich nicht. Um dem verfassungsrechtlichen Bestimmtheitsgebot zu entsprechen und die Verhältnismäßigkeit der Behördentätigkeit sicherzustellen, ist diesen genau vorzugeben, welche Datenarten sie wann speichern dürfen.

Zu § 6 Abs 4a bis 4d – mehr Datentransfers der Sicherheits- und Personenstandsbehörden als nötig und nähere Umstände der Datentransfers unklar:

Es bestehen Zweifel, die auch durch die Erläuterungen nicht ausgeräumt werden, ob es tatsächlich erforderlich und damit verhältnismäßig ist, dass Sicherheits- und Personenstandsbehörden alle nur denkbaren Änderungen von Eintragungsdaten in ihren Registern der Stammzahlenregisterbehörde zu melden haben. Für den Zweck einer E-ID erscheint dies überschießend.

Wie der Datenschutzrat dazu in seiner Stellungnahme monierte, wären *„die relevanten Änderungen daher entweder entsprechend zu konkretisieren oder es wäre unter Hinweis auf den Verhältnismäßigkeitsgrundsatz ausführlich zu begründen, aus welchen Gründen alle Änderungen der Eintragungsdaten erforderlich sind. Unklar ist auch, was eine Übermittlung „im Wege eines Änderungszugriffs" sein soll. Sollte damit die Möglichkeit eines direkten Zugriffs der Sicherheits- und Personenstandsbehörden zum Zweck der Vornahme der Änderung beabsichtigt sein, wäre die datenschutzrechtliche Rollenverteilung näher darzulegen".*

In § 6 Abs 4b ist zudem zu konkretisieren, welche „sonstigen Verantwortlichen des öffentlichen Bereichs" Daten übermitteln müssen. Der Datenschutzrat weist in seiner Stellungnahme unmissverständlich darauf hin, dass *„eine völlig undifferenzierte Verpflichtung aller Verantwortlichen des öffentlichen Bereichs zur Übermittlung aller Änderungen der Eintragungsdaten nicht dem Determinierungsgebot für eine gesetzliche Eingriffsnorm nach § 1 Abs 2 DSG (vgl. etwa VfSlg 16.369/2001 und 18.146/2007) und auch wohl auch nicht Art 18 B-VG" entspricht.*

Auch aus § 6 Abs 4c geht nicht hervor, welche personenbezogenen Daten die Stammzahlenregisterbehörde anderen Behörden zu welchem konkreten Zweck übermitteln darf.

Sollten in § 6 Abs 4d mit den „datenqualitätssichernden Maßnahmen“ weitere Datenverarbeitungen verbunden sein, sind diese konkret zu benennen.

Zu § 14 Abs 3 und § 14a Abs 2 – Verständlichkeit der Normen verbessern und Verifizierung „weiterer Merkmale“ nur mit DSGVO-konformer Einwilligung der Betroffenen:

Der Sinngehalt beider Bestimmungen ist schwer verständlich. Offengelassen wird überdies, ob es sich bei der erwähnten Einwilligung der Betroffenen um eine Einwilligung gemäß der DSGVO handelt. Aus BAK-Sicht ist unbedingt ein Verweis auf Art 4 Z 11 DSGVO im Gesetz selbst anzubringen. Mit Blick auf die kaum verständliche Formulierung beider Absätze wird sicherheitshalber auch darauf hingewiesen, dass eine datenschutzrechtliche Einwilligung „eine für den bestimmten Fall und in informierter Weise abgegebene Willenserklärung“ sein muss.

Dabei ist vor allem dem Nachweis der Freiwilligkeit der Einwilligung besonders Rechnung zu tragen. Kommerzielle Anbieter, die eine E-ID verlangen, müssen KonsumentInnen auch andere Wege einer Abklärung ihrer Identität sowie „sonstiger Merkmale“ anbieten. Um Beispiele aus den Erläuterungen aufzugreifen, wäre es nicht akzeptabel, wenn kommerzielle Anbieter etwa die Mitgliedschaft in einem Autofahrerclub, aufrechte Versicherungsverhältnisse, den Wohnort etc ausschließlich im Wege der E-ID erheben wollten. Außerdem ist das Selbstbestimmungsrecht von KonsumentInnen zu achten: es dürfen keinesfalls andere Rechtsgrundlagen der DSGVO für diese Verarbeitungen (etwa überwiegende berechtigte Interessen, gesetzliche Anordnung in diversen Materiengesetzen) herangezogen werden.

Es ist konkret anzuführen, was „nach Maßgabe technischer Möglichkeiten“ bedeutet, welche weiteren Merkmale in die Personenbindung eingefügt werden dürfen und welcher Register des öffentlichen oder privaten Bereichs die Stammzahlenregisterbehörde dabei heranziehen darf.

Zu § 18 Abs 2 und 3 – Zuverlässigkeitskriterien fehlen

Der Innenminister wird ermächtigt, Dritten – wohl Unternehmen, Behörden – die Nutzung des E-ID-Systems zu eröffnen. Diese lapidare Ermächtigung ist völlig unzureichend: es ist festzulegen, welchen Dritten unter welchen Voraussetzungen zu welchem konkreten Zweck die Nutzung des E-ID-Systems ermöglicht werden kann.

Außerdem braucht es ausreichend bestimmte Kriterien für die Zuverlässigkeitsprüfung Dritter. Die Möglichkeit einer Anfrage an die Datenschutzbehörde, ob Dritte in den letzten 5 Jahren Datenschutzrecht gebrochen haben, kann nicht das einzige Kriterium sein.
Es ist im Übrigen untauglich, da die DSB keine Daten zu diesem Zweck erhebt und kein Verwaltungsstrafregister führt.

Aus der Verordnungsermächtigung gemäß § 18 Abs 3 geht auch nicht hervor, welche Daten von den Dritten vor ihrer Freischaltung für das e-ID System verlangt werden können.
Die Antragsvoraussetzungen müssen bereits aus dem Gesetz hervorgehen. So verlangt der VfGH, dass eine Ermächtigungsnorm iSd § 1 Abs 2 DSG ausreichend präzise – also für jedermann vorhersehbar – bezeichnen muss, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist (VfSlg 16.369/2001 und 18.146/2007).

Zu § 25 Abs 2 – datenschutzkonformer Pilotbetrieb:

Es wird darauf aufmerksam gemacht, dass auch der bloße Pilotbetrieb, soweit dabei personenbezogenen Daten herangezogen werden, der DSGVO entsprechen muss.

Änderung des Passgesetzes 1992

Zu § 22b Abs 4a – Übermittlungserlaubnis der Passbehörden verfassungskonform präzise ausgestalten:

Passdaten dürften demnach auf Anfrage an Behörden und Gerichte übermittelt werden, sofern diese die Identität einer Person festzustellen haben und „dies anders nicht in der nach den Umständen gebotenen Zeit möglich ist."

Diese Übermittlungsbefugnis ist zu pauschal, zu weit und entspricht nicht annähernd dem Bestimmtheitsgebot des Art 18 B-VG. Betroffene haben überdies Anspruch darauf, dass möglichst schonend in ihre Datenschutzrechte eingegriffen wird. Es ist datenschutzverträglicher, Betroffene zunächst um Selbstauskunft und Vorlage eines Ausweises zu ersuchen, bevor ein Datentransfer durch Passbehörden in Gang gesetzt wird.

Unterzeichner	Bundeskammer für Arbeiter und Angestellte
Datum/Zeit-UTC	11.10.2020 21:52
Prüfhinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.