REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für Digitalisierung und Wirtschaftsstandort

Per Mail:
post.i2_19@bmdw.gv.at

BMJ - StS DS (Stabsstelle Bereich Datenschutz)
Kompetenzstelle A (Geschäftsstelle des Datenschutzrates)

dsr@bmj.gv.at
+43 1 52152 2918
Museumstraße 7, 1070 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an dsr@bmj.gv.at zu richten.

Geschäftszahl: 2020-0.623.605

Entwurf eines Bundesgesetzes, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden

Der **Datenschutzrat** hat in seiner 252. Sitzung am 28. September 2020 **einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

Laut den Erläuterungen zum gegenständlichen Entwurf wurden mit der Novelle des E-Government-Gesetzes (BGBl. I Nr. 121/2017) die gesetzlichen Rahmenbedingungen für die Weiterentwicklung des Konzepts Bürgerkarte hin zum E-ID (Elektronischen Identitätsnachweis) kundgemacht. Die Anwendbarkeit dieser Bestimmungen beginnt jedoch gemäß § 24 Abs. 6 E-GovG, idF BGBl. I Nr. 121/2017 erst mit Vorliegen der technischen und organisatorischen Voraussetzungen für den Echtbetrieb des E-ID. Dieser Zeitpunkt ist vom Bundesminister für Inneres im Bundesgesetzblatt kundzumachen. Dies ist bis dato nicht erfolgt, da die Voraussetzungen für den Echtbetrieb des E-ID noch nicht vorliegen.

Die Vorarbeiten und Begleitmaßnahmen für den Pilotbetrieb des E-ID gemäß § 25 Abs. 2 E-GovG sowie die Weiterentwicklung der damit verbundenen Technologie bedingen im Vorfeld des Echtbetriebs noch kleinere Adaptierungen und Ergänzungen des rechtlichen Rahmens. So muss beispielsweise für die smartphone-basierte Verwendung des E-ID zusätzlich eine sicherheitstechnisch gleichwertige Umsetzung ausdrücklich ermöglicht werden, um die Nutzung durch den User insbesondere bei Apps zu vereinfachen. Weiters sollen zur Erweiterung der Nutzungsmöglichkeiten des E-ID künftig auch Attribute aus

Registern von Verantwortlichen des privaten Bereichs über das System des E-ID (freiwillig und ausschließlich bei Einwilligung des Betroffenen) Dritten zur Verfügung gestellt werden können. Vorerst steht jedoch die Nutzung von Attributen aus Registern von Verantwortlichen des öffentlichen Bereichs weiterhin im Fokus, sodass Register von Verantwortlichen des privaten Bereichs erst in einem nächsten Schritt technisch angebunden werden sollen. Nichtsdestotrotz ist es vor allem aus verwaltungsökonomischen Gründen ratsam, die Rechtsgrundlage bereits in dieser Novelle vorzusehen. Weiters sollen im Zuge der Registrierung des E-ID und bei Änderungen der Eintragungsdaten im Ergänzungsregister für natürliche Personen (ERnP) zur Steigerung der Datenqualität auch Anpassungen vorgenommen werden. Schließlich sollen die im Zuge des Pilotbetriebs ausgestellten E-ID auch über den Zeitraum des Pilotbetriebs hinaus weiterverwendet und die zugehörigen Registrierungsdaten weiterhin verarbeitet werden dürfen.

II. Datenschutzrechtliche Bemerkungen

A) Grundsätzliches

Vorweg ist anzumerken, dass der Entwurf großteils Regelungen enthält, die sich spezifisch auf die Abbildung komplexer technischer Vorgänge im Bereich des E-Governments (insbesondere die E-ID) beziehen. Inwieweit diese technischen Vorgänge erforderlich sind, stellt keine originär datenschutzrechtliche Frage dar und kann daher auch nicht abschließend beurteilt werden.

Vor dem Hintergrund der komplexen technischen Regelungsmaterie erweisen sich diverse Bestimmungen des Entwurfes als **sehr schwer verständlich** und sollten im Sinne der Rechtsklarheit **überarbeitet und umformuliert werden**.

B) Artikel 1 (Änderung des E Government-Gesetzes)

Zu Z 3 (§ 2 Z 10a):

Aus den Erläuterungen und den Ausführungen der informierten Vertreter im Datenschutzrat geht hervor, dass für eine Nutzung des EID zumindest unter bestimmten Voraussetzungen bei der Nutzung von Mobilgeräten die Identifikation der Nutzer mittels biometrischer Merkmale erforderlich ist. Diese Identifikation erfolge unter Nutzung des entsprechenden Sicherheitsmoduls des Endgeräts des Nutzers.

Der Datenschutzrat weist darauf hin, dass es sich bei biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person um besonders schützenswerte Daten iSd Art 9 DSGVO handelt. Entsprechend sollte sichergestellt werden, dass im Sinne der **Datenminimierung** und Gleichbehandlung von Nutzern, die einer Nutzung biometrischer Identifikationsmerkmale zu Zwecken der Identifizierung nicht zustimmen oder deren Geräte eine solche nicht unterstützen, eine **alternative Nutzung ohne Verwendung besonderer Datenkategorien** ermöglicht wird. Die informierten Vertreter haben darüber hinaus im Rahmen der Sitzung des Datenschutzrates zugesagt, dass hinsichtlich einer derartigen Verwendung besonders schützenswerter Daten eine Datenschutz-Folgenabschätzung gem. Art 35 DSGVO durchgeführt werden wird.

Soweit im Zusammenhang mit dieser Verarbeitung auf Verarbeitungsergebnisse Dritter (z.B. Betriebssystemhersteller, Hersteller von Mobilgeräten) zurückgegriffen wird, sollte einerseits die Sicherheit derartiger Verarbeitungen überprüft und geklärt werden, ob es sich dabei um eine Auftragsverarbeitung handelt oder auf Basis welcher anderen Rechtsgrundlage die Datenbereitstellung erfolgt sowie ob es im Zuge dieser Datenverarbeitungen zu Datenübermittlungen in Drittstaaten wie insbesondere die USA erfolgen.

Zu Z 5 (§ 4 Abs. 5):

Es erscheint unklar, mit **welchen technischen Möglichkeiten welche weiteren Merkmale** von Verantwortlichen des öffentlichen oder privaten Bereichs eingefügt werden können. Dies sollte **im Gesetz konkreter** geregelt werden.

Weiters sollte **bereits im Gesetz** – etwa durch einen Verweis auf Art. 4 Z 11 DSGVO – klargestellt werden, ob die **Einwilligung** des E-ID-Inhabers auch eine datenschutzrechtliche Einwilligung gemäß Art. 4 Z 11 DSGVO darstellt und demzufolge an die diesbezüglichen unionsrechtlichen Voraussetzungen gebunden ist.

Zu Z 6 (§ 4a Abs. 3 und 4):

Der Zweck der **Speicherdauer von 30 Tagen** gemäß § 4a Abs. 3 sollte näher erläutert werden. Auf den **Verhältnismäßigkeitsgrundsatz** gemäß § 1 Abs. 2 DSG und die **Grundsätze der Datenminimierung und Speicherbegrenzung** (Art. 5 DSGVO) wird hingewiesen.

In § 4a Abs. 4 sollte geregelt werden, **wie lange** die von der Behörde eingeholten Informationen und Dokumente **zu speichern sind**. Auch diesbezüglich wird auf die oben genannten Grundsätze, insbesondere den Verhältnismäßigkeitsgrundsatz, hingewiesen. Es

sollte zudem deutlich klarer geregelt werden, **welche personenbezogenen Daten in diesen Informationen und Dokumenten** verarbeitet werden und wozu eine derart weitreichende Befugnis der Behörde zur Einholung von Informationen und Dokumenten nur für die Identitätsfeststellung unbedingt erforderlich ist.

Zu Z 7 (§ 4b Abs. 2 bis 5):

Hinsichtlich der Beschränkung von Rechten der betroffenen Person in § 4b Abs. 2 wird auf die Vorgaben des Art. 23 DSGVO hingewiesen. Insbesondere wird auf die **Anforderungen an die Gesetzgebungsmaßnahme** gemäß Art. 23 Abs. 2 DSGVO hingewiesen. Bloße Ausführungen in den Erläuterungen reichen wohl nicht aus, um diesen Anforderungen gerecht zu werden. **Die gesetzliche Regelung ist daher in diesem Sinne zu ergänzen und zu präzisieren.**

In § 4b Abs. 3 ist klarzustellen, **welche personenbezogenen Daten konkret verarbeitet werden.**

Zu Z 10 (§ 6 Abs. 4a bis 4d):

1. Zu § 6 Abs. 4a ist anzumerken, dass die Übermittlung grundsätzlich an den **Verantwortlichen** (die Stammzahlregisterbehörde) **im Wege des Auftragsverarbeiters** erfolgt. Dies sollte auch legistisch derart abgebildet werden.

In diesem Zusammenhang ist auch unklar, ob hier tatsächlich **alle** Änderungen der Eintragungsdaten für den hier vorliegenden Zweck erforderlich sind (siehe auch diesbezüglich den **Verhältnismäßigkeitsgrundsatz** gemäß § 1 Abs. 2 DSG). Die relevanten Änderungen wären 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.

2. In § 6 Abs. 4b wäre jedenfalls zu **konkretisieren**, welche „sonstige[n] Verantwortliche[n] des öffentlichen Bereichs“ Daten übermitteln müssen. Eine völlig undifferenzierte Verpflichtung **aller** Verantwortlichen des öffentlichen Bereichs zur Übermittlung **aller** Änderungen der Eintragungsdaten entspricht wohl nicht dem Determinierungsgebot für eine gesetzliche Eingriffsnorm nach § 1 Abs. 2 DSG (vgl. etwa VfSlg. 16.369/2001 und

18.146/2007) und wohl auch nicht Art. 18 B-VG. Zudem wäre eine solche weitreichende Übermittlungsverpflichtung auch in kompetenzrechtlicher Hinsicht zu prüfen. Sichergestellt werden sollte, dass Eintragungsdaten, die vom Betroffenen selbst stammen, nicht ohne seine Kenntnis verändert werden. Im Übrigen wird auf die obigen Anmerkungen zu § 6 Abs. 4a verwiesen.

3. Aus § 6 Abs. 4c geht nicht hervor, **welche personenbezogenen Daten zu welchem konkreten Zweck** übermittelt werden. Die Regelung wäre daher entsprechend zu konkretisieren.

4. In § 6 Abs. 4d sollte geregelt werden, welche Datenverarbeitungen mit den **„datenqualitätssichernden Maßnahmen"** konkret verbunden sind. Im Übrigen sollte im Gesetz klargestellt werden, wessen **Auftragsverarbeiter** gemeint ist.

Zu den Z 13 (§ 14 Abs. 3) und 14 (§ 14a Abs. 2):

§ 14 Abs. 3 und § 14a Abs. 2 sollten verständlicher formuliert werden. Offen lässt die Bestimmung insbesondere auch, ob es sich bei der in diesen Bestimmungen geregelten Einwilligung um eine **datenschutzrechtliche Einwilligung** gemäß Art. 4 Z 11 DSGVO handelt. Dies sollte nicht (nur) in den Erläuterungen, sondern durch einen Verweis auf Art. 4 Z 11 DSGVO **im Gesetz** klargestellt werden. Sollte es sich um eine datenschutzrechtliche Einwilligung gemäß Art. 4 Z 11 DSGVO handeln, wird im Lichte der kaum verständlichen Formulierung der beiden gegenständlichen Absätze darauf hingewiesen, dass eine datenschutzrechtliche Einwilligung eine für den bestimmten Fall und **in informierter Weise** abgegebene Willensbekundung sein muss. Unklar ist überdies, in **welche Register von Verantwortlichen des öffentlichen oder privaten Bereichs** die personenbezogenen Daten eingefügt werden können.

Zu Z 16 (§ 18 Abs. 1):

Es erscheint in § 18 Abs. 1 unklar, was mit der Formulierung „**unbeschadet der datenschutzrechtlichen Verpflichtungen des Verantwortlichen und seiner Auftragsverarbeiter**" gemeint ist. Die Regelung sollte verständlicher ausgestaltet werden.

Zu Z 17 (§ 18 Abs. 2 und 3):

Es wäre **im Gesetz** näher zu präzisieren, welchen **„Dritten"** unter welchen Auflagen und Voraussetzungen zu welchem konkreten Zweck die Nutzung des E-ID-Systems eröffnet (bzw. ermöglicht) werden kann. Offen bleibt, nach welchen Kriterien die „Zuverlässigkeits-

überprüfung“ des Dritte erfolgen soll. Der Datenschutzrat hält Zuverlässigkeitsüberprüfungen von Dritten grundsätzlich für notwendig.

Hinsichtlich der **Anfrage an die Datenschutzbehörde**, ob und über welche Anhaltspunkte sie verfügt, dass der Dritte in den letzten fünf Jahren personenbezogene Daten nicht auf diese Weise verarbeitet hat, ist darauf hinzuweisen, dass die **(unabhängige**) Datenschutzbehörde diese Daten **nicht für diese Zwecke** erhoben hat bzw. verarbeitet (gemeint offenbar im Sinne einer Art „Verwaltungsstrafregister“ für Datenschutzverstöße, wofür jedoch eine gesetzliche Grundlage fehlt). Zudem steht diese Anfrage in einem **evidenten Spannungsverhältnis mit der Unabhängigkeit der Datenschutzbehörde** (Art. 52 DSGVO und § 19 DSG) und hätte daher zu entfallen.

Im Hinblick auf die **Verordnungsermächtigung** gemäß § 18 Abs. 3 wird darauf hingewiesen, dass die Verarbeitung von personenbezogenen Daten bereits **aus der gesetzlichen Rechtsgrundlage „vorhersehbar“ sein muss** (siehe auch die Rsp des VfGH, wonach eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG [2000] 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 [vgl. etwa VfSlg. 16.369/2001 und 18.146/2007]).

Zu Z 18 (§ 18 Abs. 4 und 5):

Hinsichtlich der Regelung der Verarbeitung personenbezogener Daten in einer Verordnung gemäß § 18 Abs. 4 iVm Abs. 3 wird auf die Anmerkungen zu § 18 Abs. 3 zum Erfordernis der „Vorhersehbarkeit“ und auf die zitierte VfGH-Judikatur verwiesen.

Auch in § 18 Abs. 4, 5 und 6 ist unklar, welche „**Dritten**“ in Betracht kommen. Auf die Anmerkungen oben zu § 18 Abs. 2 und 3 wird verwiesen.

Zu Z 20 (§ 25 Abs. 2):

Es wird darauf hingewiesen, dass auch für die im **Pilotbetrieb** verarbeiteten personenbezogenen (Echt)Daten die Vorgaben der DSGVO und des DSG – etwa hinsichtlich der erforderlichen Rechtsgrundlagen – vollumfänglich zur Anwendung kommen.

C) Artikel 2 (Änderung des Passgesetzes 1992)

Zu Z 3 (§ 22b Abs. 3):

Die Erläuterungen zu § 22b Abs. 3 führen – zusammengefasst – aus, dass es aus verwaltungsökonomischen Gründen sachgerecht sei, die personenbezogenen Daten sowie aktuelle Lichtbilder von Betroffenen im IDR für Zwecke von Verfahren nach dem Passgesetz 1992 weiterzuverarbeiten, und weiterhin die Möglichkeit bestehe, ein aktuelles Lichtbild beizubringen. Es sollte in den Erläuterungen dargestellt werden, **aus welchen Regelungen sich diese alternative Möglichkeit** der Beibringung eines aktuellen Lichtbildes dann weiterhin ergibt.

Zu Z 5 (§ 22b Abs. 4a):

Die Datenübermittlung gemäß § 22b Abs. 4a ist deutlich zu weit und zu pauschal gefasst und wäre **im Gesetz** näher zu konkretisieren (auf die Ausführungen zum Determinierungsgebot oben zu § 6 Abs. 4b wird sinngemäß verwiesen).

Zur wirkungsorientierten Folgenabschätzung:

Es wäre näher zu begründen, weshalb keine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO erforderlich ist.

Für den Datenschutzrat
Der Vorsitzende:
OFENAUER
30. September 2020

Elektronisch gefertigt