Erläuterungen

I. Allgemeiner Teil

Zu Artikel 1 (Änderung des E-Government-Gesetzes):

Mit der Novelle des E-Government-Gesetzes (BGBl. I Nr. 121/2017) wurden 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.

Zu Artikel 2 (Änderung des Passgesetzes 1992):

Die vorgeschlagenen Änderungen ermöglichen zum einen den Nachweis von personenbezogenen Daten mithilfe des E-ID im Bereich des Passwesens, da eine Rechtsgrundlage für die Übermittlung dieser personenbezogenen Daten an die Stammzahlenregisterbehörde geschaffen werden soll, sofern dieser eine gesetzlich übertragene Aufgabe zukommt. Zum anderen sollen die in der Datenverarbeitung gemäß § 22b des Passgesetzes 1992, BGBl. Nr. 839/1992, bzw. in der zentralen Evidenz bzw. im Identitätsdokumentenregister (IDR), verarbeiteten Daten aus verwaltungsökonomischen Gründen für Zwecke von Verfahren nach dem Passgesetz 1992 weiterverarbeitet werden dürfen. Weiters soll die Identitätsfeststellung für Behörden und ordentliche Gerichte, sofern diese einer gesetzlich übertragenen Aufgabe dient, unter Zuhilfenahme der im IDR verarbeiteten Daten maßgeblich erleichtert werden.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes gründet sich hinsichtlich

- des Artikels 1 auf die Bedarfsgesetzgebungskompetenz für das Verwaltungsverfahren nach Art. 11 Abs. 2 B-VG, auf Art. 10 Abs. 1 Z 3 B-VG („Passwesen“) sowie Art. 10 Abs. 1 Z 7 B-VG („Meldewesen“) sowie

- des Artikels 2 auf Art. 10 Abs. 1 Z 3 B-VG („Passwesen“).

II. Besonderer Teil

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

Zu Z 1, 5, 13, 14, 15 und 16 (Inhaltsverzeichnis, § 4 Abs. 5 letzter Satz, § 14 Abs. 3 dritter Satz, § 14a Abs. 2 letzter Satz und § 18 Abs. 1):

Schon die bisherige Regelung sah vor, dass es im Rahmen der Nutzung des E-ID dem E-ID-Inhaber möglich sein soll, neben den Kernidentitätsdaten (Vorname, Familienname, Geburtsdatum) weitere Merkmale aus für die Stammzahlenregisterbehörde zugänglichen elektronischen Registern eines Verantwortlichen des öffentlichen Bereichs Dritten (Serviceanbietern) zu Verfügung zu stellen. Zugänglich für die Stammzahlenregisterbehörde bedeutet das faktische Vorhandensein der technischen

Abfragemöglichkeit, aber auch, dass eine entsprechende (materien)gesetzliche Grundlage für die Weitergabe der Merkmale aus diesem Register an die Stammzahlenregisterbehörde besteht.

Diese Möglichkeit soll nun auf für die Stammzahlenregisterbehörde zugängliche Register eines Verantwortlichen des privaten Bereichs erweitert werden, um die Nutzungsmöglichkeiten des E-ID zu erweitern und den Nutzen für E-ID-Inhaber sowie Serviceanbieter noch weiter zu erhöhen. Zugänglich ist ein solches Register für die Stammzahlenregisterbehörde nur, wenn eine geeignete technische Anbindung vorhanden ist und eine entsprechende gesonderte Rechtmäßigkeit der Verarbeitung gemäß Art. 6 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, (im Folgenden: DSGVO) – z. B. Einwilligung – für die Weitergabe der Merkmale aus diesem Register im Wege des E-ID besteht. So könnten beispielsweise Versicherungsnachweise oder Bestätigungen über Mitgliedschaften unter Nutzung der Funktion E-ID unter Kontrolle des E-ID-Inhabers berechtigten Serviceanbietern übermittelt werden. Wie bereits im allgemeinen Teil ausgeführt, soll die Möglichkeit der Nachweise von Merkmalen aus Registern von Verantwortlichen des privaten Bereichs erst in einem nächsten Schritt technisch umgesetzt werden.

Zu Z 2 (§ 1b Abs. 1):

Ein Redaktionsversehen soll durch die korrekte BGBl.-Nummer bereinigt werden.

Zu Z 3 (§ 2 Z 10a):

Es soll eine Definition für den Verwendungsvorgang des E-ID eingeführt werden. Diese soll klarstellen, dass bei der Verwendung des E-ID die Erstellung einer Personenbindung entweder so wie schon derzeit mittels qualifizierter elektronischer Signatur des E-ID-Inhabers oder alternativ mittels eines sicherheitstechnisch gleichwertigen Vorgangs ausgelöst werden kann.

Die qualifizierte Signatur wird bei der smartphone-basierten Umsetzung des Bürgerkartenkonzepts (so genannte Handy-Signatur) aktuell durch drei Faktoren ausgelöst, das Wissen des Benutzers (Passwort – Faktor 1), der Besitz des Geräts (hardwarebasiertes Element für Schlüsselaufbewahrung – Faktor 2) und eine biometrische Eigenschaft des Benutzers (aktuell Fingerabdruck und bestimmte Gesicht-Scans – Faktor 3). Der sicherheitstechnisch gleichwertige Vorgang zum Auslösen der Erstellung einer Personenbindung bei Verwendung des E-ID wird erstmalig durch eine qualifizierte Signatur des E-ID-Inhabers initiiert. Dabei wird als Sicherheitselement ein Schlüssel im hardwarebasierten Element des Geräts erstellt und der Zugriff mit einer biometrischen Eigenschaft abgesichert (äquivalent zum zweiten und dritten Faktor der qualifizierten Signatur) und durch den E-ID-Inhaber qualifiziert signiert. Dadurch entsteht eine kryptographische Bindung zwischen der qualifizierten Signatur des E-ID-Inhabers und dem erstellten Schlüssel. Die Kombination aus der kryptographischen Bindung durch die initial erstellte qualifizierte Signatur und der Verwendung des zuvor erwähnten Sicherheitselements entspricht einem sicherheitstechnisch gleichwertigen Vorgang. Das zugehörige qualifizierte Zertifikat, das für die frühere qualifizierte elektronische Signatur verwendet wurde, muss zum Zeitpunkt der jeweiligen Verwendung gültig sein.

Durch diesen alternativen Vorgang kann insbesondere die mobile Verwendung des E-ID aus Usersicht stark vereinfacht werden, ohne sicherheitstechnische Nachteile hinnehmen zu müssen.

Ob diese alternative Verwendung für ein konkretes Verfahren ausreichend ist, hängt vom jeweiligen Verfahren, demgegenüber sich der E-ID-Inhaber authentifiziert, ab. Ist beispielsweise neben der Authentifizierung zusätzlich die eigenhändige Unterschrift für das konkrete Verfahren aufgrund anderer rechtlicher Regelung erforderlich, so muss der E-ID jedenfalls mit einer qualifizierten elektronischen Signatur ausgelöst werden.

Zu Z 4 (§ 4 Abs. 4):

Sofern die Erstellung der Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers ausgelöst wird (§ 2 Z 10a erster Fall), übermittelt der qualifizierte Vertrauensdiensteanbieter (VDA) der Stammzahlenregisterbehörde die verschlüsselte Stammzahl und die dazugehörigen Sicherheitsdaten (vgl. § 4 Abs. 5 zweiter Satz). Wird der E-ID über einen sicherheitstechnisch gleichwertigen Vorgang wie nun in § 2 Z 10a zweiter Fall definiert ausgelöst, so muss die verschlüsselte Stammzahl zum E-ID dieses E-ID-Inhabers gespeichert werden, da bei dieser Methode die verschlüsselte Stammzahl nicht vom VDA übermittelt wird.

Zu Z 5, 13 und 14 (§ 4 Abs. 5 zweiter Satz, § 14 Abs. 3 zweiter Satz und § 14a Abs. 2 zweiter Satz):

§ 4 Abs. 5 soll aufgrund der neu einzuführenden Definition des § 2 Abs. 10a dahingehend angepasst werden, dass der VDA nur mehr im Falle einer tatsächlich durch eine qualifizierte elektronische Signatur ausgelöste Verwendung des E-ID die verschlüsselte Stammzahl der Stammzahlenregisterbehörde

übermittelt. Im alternativen Fall der Verwendung ist wie in § 4 Abs. 4 neu vorgeschlagen die verschlüsselte Stammzahl direkt zum E-ID des E-ID-Inhabers zu speichern. Außerdem sind nun nicht mehr Vorname, Familienname und Geburtsdatum, sondern bloß die zugehörigen Sicherheitsdaten (vgl. § 2 Z 10 geltender Fassung) vom VDA zu übermitteln. Diese Kernidentitätsdaten (Vorname, Familienname und Geburtsdatum) werden bei jeder Verwendung des E-ID unmittelbar aus dem Zentralen Melderegister (ZMR) übernommen.

Zu Z 6 (§ 4a Abs. 3 und 4):

Mit der vorgeschlagenen Regelung soll präzisiert werden, dass Inhaber eines inländischen Reisedokuments im Rahmen der Vorregistrierung eines E-ID bestimmte personenbezogene Daten den Behörden im Wege des VDA, der im Auftrag des Bundesministers für Inneres tätig wird, zur Verfügung stellen können. Die Vor- und Familiennamen, das Geburtsdatum, die Pass- oder Personalausweisnummer sowie gegebenenfalls die bekanntgegebene E-Mail-Adresse können für eine anschließende raschere Abwicklung des Registrierungsprozesses herangezogen werden, sofern der Betroffene die Registrierung eines E-ID innerhalb von 30 Tagen ab Bekanntgabe dieser Daten durchführen lässt.

In diesem Zusammenhang soll auch klargestellt werden, dass der Begriff der „inländischen Reisedokumente“ eng auszulegen ist und daher insbesondere Fremden- und Konventionsreisepässe gemäß §§ 88 ff des Fremdenpolizeigesetzes 2005 (FPG), BGBl. I Nr. 100/2005, nicht als inländische Reisedokumente gemäß dem Passgesetz 1992 zu qualifizieren sind.

Es sollen für eine Vorregistrierung darüber hinaus nur jene Inhaber eines inländischen Reisedokuments in Frage kommen, deren Gültigkeitsdauer des Reisedokuments nicht länger als sechs Jahre abgelaufen ist. Vor diesem Zeitpunkt verfügt die Registrierungsbehörde regelmäßig noch über Daten im IDR, die für die Registrierung eines E-ID weiterverwendet werden können.

Um eine sinnvolle und praxisnahe Nutzung des E-ID zu gewährleisten, soll in Abs. 4 normiert werden, dass der E-ID-Werber grundsätzlich zur Beibringung eines Lichtbilds verpflichtet ist. Diese Verpflichtung soll jene E-ID-Werber treffen, die nicht schon ohnehin aufgrund der beabsichtigten Ausstellung eines Reisedokuments ein Lichtbild beizubringen haben oder das im Rahmen der bereits erfolgten Ausstellung eines Reisedokuments beigebrachte Lichtbild zum Zeitpunkt der Registrierung des E-ID noch die Kriterien des § 4 der Passgesetz-Durchführungsverordnung (PassG-DV), BGBl. II Nr. 223/2006, erfüllt. Insbesondere darf das entsprechende Lichtbild daher nicht älter als sechs Monate sein.

Im Hinblick auf die Möglichkeit, dass auch Fremde die Registrierung eines E-ID gemäß § 4a Abs. 2 verlangen können, ist es sachgerecht, zur Überprüfung der Identität und der vorgelegten Dokumente auch die vorhandenen Datenbestände des Zentralen Fremdenregisters gemäß §§ 26 und 27 des BFA-Verfahrensgesetzes (BFA-VG), BGBl. I Nr. 87/2012, heranziehen zu können.

Zu Z 7 (§ 4b Abs. 1 bis 5):

Zu Abs. 1:

Bei den vorgeschlagenen Regelungen in Abs. 1 handelt es sich lediglich um formale Anpassungen und sollen damit keine inhaltlichen Änderungen herbeigeführt werden. In Z 1 soll klargestellt werden, dass wie bereits nach geltender Rechtslage die Registrierungsbehörde ermächtigt ist, sowohl sämtliche Vor- als auch Familiennamen im IDR zu verarbeiten. Die Ergänzung in Z 8 soll sicherstellen, dass im IDR stets das aktuelle Lichtbild verarbeitet wird.

Zu Abs. 2:

Gemäß Art. 21 Abs. 1 DSGVO hat der Betroffene das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus hat der Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen.

Ein solches, dem Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung kann jedoch gemäß Art. 23 DSGVO zur Sicherstellung einer der in Abs. 1 lit. a bis j genannten Zwecke durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung wird in § 4b Abs. 2 für sämtliche zum Zwecke der Registrierung eines E-ID verarbeiteten Daten Gebrauch gemacht.

Die Registrierung des E-ID erfolgt stets unter Verarbeitung personenbezogener Daten in der zentralen Evidenz, die Registrierungsdaten sind dem qualifizierten VDA zur Ausstellung eines qualifizierten Zertifikats zu übermitteln. E-ID-Inhaber haben das Recht, zu jedem Zeitpunkt eine vorübergehende Aussetzung sowie einen Widerruf des E-ID bei der Behörde zu verlangen. § 4a Abs. 5 verpflichtet die

Behörden zudem zur Aussetzung oder zum Widerruf eines E-ID, insbesondere, wenn sie Kenntnis vom Tod des E-ID-Inhabers oder einer drohenden Missbrauchsgefahr erlangen sowie für den Fall, dass Zweifel an der Identität des Betroffenen aufkommen. Eine Erfüllung dieser Aufgaben ist unmöglich, wenn die Daten aufgrund eines Widerspruchs des Betroffenen nicht verarbeitet werden dürfen. Den Behörden würde im Falle eines Widerspruchs jede Handlungsmöglichkeit entzogen, die missbräuchliche Verwendung – insbesondere auch die Verwendung eines E-ID mit einer zweifelhaften Identität – zu unterbinden.

Auch sonst ist es zu Beweiszwecken und zur Vermeidung allfälliger Amtshaftungsansprüche unumgänglich, dass das Bestehen eines gültigen E-ID und damit die Möglichkeit der Verwendung im Rechtsverkehr bzw. der Zeitpunkt einer Aussetzung oder eines Widerrufs von den Behörden nachvollzogen werden kann.

Die Ausübung dieser Rechte hätte zudem einen beträchtlichen Verwaltungsaufwand zur Folge, da einerseits die in § 4a Abs. 1 vorgesehene amtswegige Registrierung des E-ID rasch zu einer hohen Anzahl an E-ID-Inhabern führen wird und andererseits durch den Ausschluss des Widerspruchsrechts und des Rechts auf Einschränkung der Verarbeitung in § 22b Abs. 6 Passgesetz 1992 innerhalb eines Registers unterschiedliche datenschutzrechtliche Rahmenbedingungen geschaffen würden.

Zur Gewährleistung eines geordneten Vollzugs des E-Government-Gesetzes durch die Registrierungsbehörden gemäß § 4a ist demnach der Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO zwingend erforderlich. Die in § 4a Abs. 1 vorgesehene Möglichkeit eines „Opt-Outs“ bleibt unberührt.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an behördliche Register oder Dateisysteme, ausschließlich rechtmäßig verarbeitete personenbezogene Daten zu enthalten, umgehend zu löschen und soll es nicht möglich sein, dass der Betroffene lediglich die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. b und lit. c DSGVO verlangt.

Den für den Ausschluss des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung einschlägigen Vorgaben des Art. 23 Abs. 2 DSGVO wird entsprechend Rechnung getragen. So ergeben sich aus den gesetzlichen Vorgaben zur Verarbeitung von personenbezogenen Daten nach diesem Bundesgesetz für den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO insbesondere sowohl der Umfang der vorgenommenen Beschränkung und die Kategorien der betreffenden personenbezogenen Daten als auch die für deren Verarbeitung Verantwortlichen und Zwecke sowie die jeweiligen Speicherfristen. Der Ausschluss des Rechts auf Widerspruch gegen die Verarbeitung von personenbezogenen Daten bezieht sich überdies selbstverständlich ausschließlich auf jene Daten, die in Übereinstimmung mit den gesetzlichen und unionsrechtlichen Vorgaben in rechtskonformer Weise verarbeitet werden. Den Betroffenen bleibt es zudem auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen oder unrechtmäßig verarbeiteten personenbezogenen Daten oder personenbezogenen Daten, deren Verarbeitung für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig ist, von ihrem Recht auf Berichtigung und Löschung gemäß den Art. 16 bis 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß Art. 18 und 21 DSGVO entsteht für den Betroffenen daher auch kein Rechtsschutzdefizit.

Als grundrechtsschützende Maßnahme und in Umsetzung des Art. 23 Abs. 2 lit. h DSGVO ist im letzten Satz vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind. Ausdrücklich steht es den Registrierungsbehörden dabei frei, diese Information nicht an jeden einzelnen Betroffenen individuell, sondern an „die Betroffenen“ in deren Gesamtheit zu richten. Die Information kann daher auch in allgemeiner Weise erteilt werden (z. B. auf einer Homepage).

Die Ausführungen lassen erkennen, dass das in der DSGVO vorgesehene Recht auf Widerspruch sowie das Recht auf Einschränkung der Verarbeitung in einem Spannungsverhältnis zur gesetzlich angeordneten Datenverarbeitung stehen. Die Bestimmung stellt demzufolge eine ausgewogene Abwägung zwischen den administrativen Interessen sowie dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar und soll den Vollzug der Registrierungsbehörden sowie die Funktionalität und die ordnungsgemäße Führung der zentralen Evidenz gewährleisten.

Zu Abs. 3:

An dieser Stelle wird zur Nachvollziehbarkeit der Registrierung eines E-ID in Anlehnung an die Ausstellung von Reisedokumenten nach dem Passgesetz 1992 (§ 22a Abs. 5 Passgesetz 1992) vorgeschlagen, dass die Registrierungsbehörden im Identitätsdokumentenregister die Daten der

vorgelegten Urkunden, mit welchen die Registrierungsdaten nachgewiesen werden, gemeinsam mit den darauf Bezug habenden personenbezogenen Daten des Betroffenen verarbeiten, also auch beim jeweiligen Eintrag des Betroffenen speichern dürfen.

Zu Abs. 4:

§ 14 DSG 2000 sah vor Inkrafttreten der DSGVO unter anderem vor, dass Protokolldaten über tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen drei Jahre lang aufzubewahren sind, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist. Durch den Entfall des bisherigen § 14 DSG 2000 durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, und den Umstand, dass die DSGVO von spezifischen Regelungen betreffend die Protokollierung Abstand nimmt, wird vorgeschlagen, dass auch weiterhin Protokoll geführt wird, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Dabei soll die ursprünglich in § 14 Abs. 5 DSG 2000 enthaltene Protokollierungsdauer von drei Jahren beibehalten werden.

Zu Abs. 5:

Die Löschungsregelung in Abs. 5 wird vor dem Hintergrund des datenschutzrechtlichen Grundsatzes der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO vorgeschlagen: Die bekanntgegebene Zustelladresse wird beispielsweise nur bis zum vollständigen Abschluss der Registrierung des E-ID benötigt, insbesondere um dem Betroffenen die Zugangsdaten zum E-ID zu übermitteln. Sobald ein Betroffener sein E-ID-Zertifikat widerruft, besteht auch kein Grund mehr für die Aufbewahrung des zugehörigen Identitätscodes.

Sonstige gemäß Abs. 1 verarbeitete Daten sind spätestens drei Jahre nach Widerruf des E-ID zu löschen. Diese Regelung soll die Registrierung von Betroffenen, die sich erneut für einen E-ID entscheiden, dahingehend erleichtern, dass die eindeutige Identitätsfeststellung im Sinne des § 4a Abs. 4 durch die Registrierungsbehörde unter Verwendung der bereits in der zentralen Evidenz verarbeiteten Daten (insbesondere auch des Lichtbilds) erfolgen kann. Dadurch kann eine wesentliche Verwaltungserleichterung erzielt werden und können die Betroffenen von einer raschen und unkomplizierten Registrierung des E-ID profitieren. Die Aufbewahrung der personenbezogenen Daten ist zudem im Hinblick auf E-ID, die aufgrund von missbräuchlicher Verwendung oder zweifelhaften Identitäten widerrufen wurden, erforderlich. Diese Information muss für sämtliche Behörden verfügbar sein, um die erneute Registrierung eines E-ID in diesen Fällen zu vermeiden.

Zu Z 8 (§ 6 Abs. 1):

Es soll eine sprachliche Anpassung vorgenommen werden, um besser zum Ausdruck zu bringen, dass die eindeutige Identifikation von natürlichen Personen im E-ID letztlich nicht durch die Stammzahl selbst, sondern durch eine Ableitung auf Basis der Stammzahl mittels bereichsspezifischen Personenkennzeichen erfolgt.

Zu Z 9 (§ 6 Abs. 4):

Der bisherige vierte Satz dieser Bestimmung kann entfallen, da die Eintragungsdaten in der zu novellierenden Ergänzungsregisterverordnung im Detail festgelegt werden.

Zu Z 10 (§ 6 Abs. 4a bis 4d):

Das Bundesministerium für Inneres verfolgt seit jeher das Ziel, die bestmögliche Datenqualität in den von ihm (in der Rolle des Verantwortlichen oder des Auftragsverarbeiters) geführten Registern zu gewährleisten. Erfahrungen aus der Verwaltungspraxis haben gezeigt, dass die Herausforderungen im Hinblick auf die Richtigkeit und die Aktualität der Daten im Ergänzungsregister für natürliche Personen (ERnP) vor allem durch Eintragungen von Sicherheits- und Personenstandsbehörden bewältigt werden können. Sofern diese Behörden beispielsweise durch ein laufendes Verwaltungsverfahren von geänderten Eintragungsdaten Kenntnis erlangen, werden diese die Änderung in der Regel zuerst in ihrer eigenen Fachapplikation eintragen und sollen diese dem ERnP in einem nächsten Schritt über eine technische Schnittstelle – den sogenannten Änderungszugriff – übermitteln.

Erlangt ein sonstiger Verantwortlicher des öffentlichen Bereichs etwa durch ein laufendes Verwaltungsverfahren Kenntnis von geänderten Eintragungsdaten des ERnP, hat er dies nach Maßgabe der technischen Möglichkeiten dem Auftragsverarbeiter zu melden. Letzterer verständigt in weiterer Folge die ursprünglich eintragende Stelle, sofern es sich hierbei um eine Sicherheits- oder Personenstandsbehörde handelt, die in weiterer Folge nach Abs. 4a erster Satz vorzugehen hat. Ansonsten hat der Auftragsverarbeiter die Änderung der Eintragungsdaten im ERnP selbst vorzunehmen.

Damit auch jene Verantwortliche des öffentlichen Bereichs, die Daten von im ERnP eingetragenen Betroffenen verarbeiten, von den unter Einhaltung hoher Qualitätsansprüche geänderten Eintragungsdaten profitieren können, soll in Abs. 4c ein Änderungsdienst zur Verfügung gestellt werden. Ein derartiger Änderungsdienst, der auf Verlangen der Verantwortlichen des öffentlichen Bereichs die gemäß § 6 Abs. 4a und 4b geänderten Eintragungsdaten übermittelt, soll gewährleisten, dass diese stets über aktuelle Daten zum Betroffenen verfügen.

Die vorgeschlagene Regelung in Abs. 4d verfolgt bereits wie die vorbildhafte Bestimmung in § 16 Abs. 7 des Meldegesetzes 1991 (MeldeG), BGBl. Nr. 9/1992, das Ziel, eine hohe Datenqualität im ERnP zu gewährleisten und insbesondere sicherzustellen, dass der zu einer Person zu verarbeitende Datensatz einerseits nicht mehrfach im ERnP erfasst wird sowie andererseits zusätzlich zum Eintrag im ERnP nicht auch ein aktueller Eintrag im ZMR besteht. Ein Eintrag im ERnP ist nämlich nur in jenen Fällen erforderlich, als der Betroffene über keinen aktuellen Wohnsitz im Inland verfügt und demnach zum Betroffenen auch kein aktueller Eintrag im ZMR vorhanden ist.

Zu Z 11 und 12 (§ 14 Abs. 1 und 2):

Bei der Verwendung der Funktion E-ID im privaten Bereich kann schon bisher ein bPK gebildet werden, wobei für die Errechnung des bPK anstelle der Bereichskennung die Stammzahl des Verantwortlichen des privaten Bereichs herangezogen wird. Dies ist somit für juristischen Personen, Vereine oder im Ergänzungsregister eingetragene Betroffene, die eine Stammzahl für den Errechnungsvorgang zur Verfügung stellen können, möglich. Um auch natürlichen Personen, die Möglichkeit zu eröffnen als Serviceanbieter unter Einsatz einer E-ID tauglichen technischen Umgebung zu fungieren, soll anstelle der Stammzahl auch das bPK des Verantwortlichen des privaten Bereichs für die bPK-Errechnung herangezogen werden dürfen.

Zu Z 16 (§ 18 Abs. 1):

Bei der vorgeschlagenen Regelung im Schlussteil handelt es sich um eine terminologische Anpassung an die DSGVO.

Wie bisher ist im Rahmen des E-ID-Systems sicherzustellen, dass die Protokollierung der Datenübermittlung aus dem E-ID-System im Auftrag des E-ID-Inhabers lediglich dem jeweiligen Betroffenen zugänglich ist. Die Protokollierung soll jedoch im Einklang mit den datenschutzrechtlichen Vorgaben der DSGVO auch für den Verantwortlichen und dessen Auftragsverarbeiter ersichtlich sein, da diese nur auf diesem Wege etwaigen Auskunfts- oder Löschungsersuchen der Betroffenen nachkommen können.

Zu Z 17 (§ 18 Abs. 2 und 3):

In Anlehnung an die Registrierung von Verantwortlichen des öffentlichen Bereichs gemäß § 10 Abs. 1 sollen sich auch Dritte (Serviceanbieter), folglich Verantwortliche des privaten Bereichs, für die Nutzung des E-ID-Systems beim Bundesminister für Inneres zu registrieren haben, der in weiterer Folge auch über die Eröffnung oder Unterbindung der Nutzung des E-ID-Systems entscheidet.

Voraussetzung für eine Teilnahme am E-ID-System ist wie bisher die Verarbeitung personenbezogener Daten nach Treu und Glauben. Um dies zu gewährleisten soll in Abs. 2 eine Mitwirkungspflicht des Dritten normiert werden, dass dieser dem Bundesminister für Inneres jeden Umstand bekanntzugeben hat, der einer Verarbeitung nach Treu und Glauben entgegensteht. Zu diesem Zweck soll auch eine Anfragemöglichkeit an die Datenschutzbehörde vorgesehen werden, da abgesehen vom Dritten nur diese eine verlässliche Auskunft darüber geben kann, ob der Dritte innerhalb der vergangenen fünf Jahre personenbezogene Daten auf diese Art und Weise verarbeitet hat. Bei einer diesbezüglichen Mitteilung der Datenschutzbehörde sollen lediglich vorhandene Informationen aus bereits rechtskräftig abgeschlossenen Verfahren übermittelt werden.

Eine weitere wesentliche Voraussetzung für die Eröffnung der Nutzung durch den Bundesminister für Inneres ist die Glaubhaftmachung eines eigenen Zwecks. Ein solcher Zweck kann beispielsweise in einem Vorhaben eines Verkehrsverbunds bestehen, seinen Fahrgästen mit Hauptwohnsitz in einer bestimmten Gemeinde ein ermäßigtes Jahresticket anzubieten. Vom glaubhaft gemachten Zweck hängen naturgemäß auch die Datenarten ab, die vom Betroffenen angefordert werden. Es ist zu beachten, dass die bloße Weitergabe von empfangenen Datensätzen für eine solche Glaubhaftmachung nicht ausreicht.

Zu Z 18 (§ 18 Abs. 4 bis 6):

Zur besseren Übersicht sollen die bisher in Abs. 3 vorhandenen Verordnungsermächtigungen auf zwei Absätze aufgeteilt werden.

Aus Sicht des Bundesministeriums für Inneres ist es erforderlich, die Verordnungsermächtigungen insoweit zu ergänzen, als die zur Registrierung erforderlichen Angaben sowie die für eine Registrierung

gemäß Abs. 2 in Frage kommenden Dritten einschließlich der zu verrechnenden Kostenersätze in der Verordnung näher zu bestimmen sind.Für die Übermittlung der für die Nutzung des E-ID-Systems offenstehenden Datenarten bedarf es zusätzlich zu § 18 Abs. 1 einer diesbezüglichen Rechtsgrundlage im jeweiligen Materiengesetz. Für den Fall, dass diese Datenarten nicht bereits durch die Gesetzesbestimmung ausreichend konkretisiert wurden, soll mit der vorgeschlagenen Verordnungsermächtigung ermöglicht werden, dass der für die jeweilige Datenverarbeitung zuständige Bundesminister diese Datenarten mit Verordnung konkretisieren kann. Dabei sollen mit Verordnung jedoch lediglich Identitätsdaten (z. B. Vor- und Familiennamen sowie Geburtsdatum), Informationen zu Berechtigungen eines Betroffenen (z. B. Daten eines Reisedokumentes) oder Umstände, die der Betroffene nachweisen möchte (z. B. Hauptwohnsitz) festgelegt werden. Der Bundesminister für Inneres könnte beispielsweise die für die Verwendung der Funktion E-ID aus dem ZMR zur Verfügung stehenden Datenarten, die gemäß § 16a Abs. 4 MeldeG an die Stammzahlenregisterbehörde zur Erfüllung der gesetzlich übertragenen Aufgabe in § 18 Abs. 1 E-GovG übermittelt werden, durch Verordnung präzisieren.

Um die im Rahmen der Registrierung angegebenen Informationen aktuell zu halten, soll in Abs. 5 eine Meldepflicht für Dritte gemäß § 18 Abs. 1 Z 2 eingeführt werden, sodass eine Änderung dieser Informationen unverzüglich dem Bundesminister für Inneres bekanntzugeben ist. Soweit es sich beim Dritten um einen Teilnehmer des Unternehmensserviceportals (USP) gemäß § 5 des Unternehmensportalgesetzes (USPG), BGBl. I Nr. 52/2009, handelt, sind derartige Änderungen im Wege des Unternehmensserviceportals bekanntzugeben.

Darüber hinaus soll für jene Fälle, in denen das E-ID-System über einen Zeitraum von fünf Jahren nicht genutzt wird, vorgesehen werden, dass die durch den Dritten im Rahmen der Registrierung angegebenen Daten unwiderruflich gelöscht werden. Mit Ablauf dieses Zeitraums ist wohl in der Regel davon auszugehen, dass kein Interesse des Dritten mehr an der Nutzung des E-ID-Systems besteht.

Da wie bereits erwähnt die anzufordernden Datenarten maßgeblich vom glaubhaft gemachten eigenen Zweck abhängen, soll in Abs. 6 vorgesehen werden, dass Dritte eine Änderung dieses Zwecks oder den Umstand, dass sie diesen Zweck nicht mehr verfolgen wollen oder dürfen, dem Bundesminister für Inneres zu melden haben. Für den Fall, dass der Dritte den glaubhaft gemachten Zweck nicht mehr verfolgen will oder darf, steht es ihm jederzeit frei, die Nutzung des E-ID-Systems von sich aus vorübergehend stillzulegen und zu einem späteren Zeitpunkt wiederaufzunehmen. Der Bundesminister für Inneres hat nach Eingang der Meldung zu überprüfen, ob eine dauerhafte Unterbindung der Nutzung notwendig erscheint. Wurde die Nutzung schließlich unterbunden und besteht seitens des Dritten der Wunsch, die Nutzung des E-ID-Systems wiederaufzunehmen, ist der gesamte Registrierungsprozess zu wiederholen und werden die Voraussetzungen für eine Eröffnung der Nutzung erneut überprüft.

In Entsprechung zur Mitwirkungspflicht vor Eröffnung der Nutzung des E-ID-Systems, soll Dritten in Fällen der Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO eine Meldepflicht gegenüber dem Bundesminister für Inneres auferlegt werden. Der Inhalt der Meldung hat dabei dem Umfang der entsprechenden Meldung an die Datenschutzbehörde zu entsprechen. Im Falle einer Meldung iSd Z 3 soll den Dritten darüber hinaus eine Stilllegungspflicht hinsichtlich der Nutzung des E-ID treffen. Diese ist insofern eingeschränkt, als sie nur jene Datenverarbeitungen bzw. Anwendungen betrifft, die im Zusammenhang mit der Nutzung des E-ID-Systems stehen. Sie betrifft folglich nicht sämtliche Datenverarbeitungen des Dritten. Eine weitere Einschränkung ergibt sich aus Art. 33 Abs. 1 DSGVO, wonach eine Meldepflicht einer Verletzung des Schutzes personenbezogener Daten an die Datenschutzbehörde nur insofern besteht, als diese voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Zudem handelt es sich bei der Stilllegung des E-ID-Systems um eine aus datenschutzrechtlichen Gründen gebotene Einschränkung der Nutzung: Die Stilllegung kann durch Dritte selbständig wieder rückgängig gemacht werden, sobald hinsichtlich der Verletzung des Schutzes personenbezogener Daten kein Risiko mehr für die Rechte und Freiheiten natürlicher Personen besteht.

Zu Z 19 (§ 24 Abs. 9):

Die Notwendigkeit einer Vorlaufzeit für die technischen Anpassungen macht die spätere Anwendbarkeit der Bestimmungen erforderlich. Lediglich § 1b Abs. 1, § 6 Abs. 4 und § 25 Abs. 2 sollen bereits ab dem Zeitpunkt des Inkrafttretens Anwendung finden, um die rechtzeitige Erlassung der zu adaptierenden Verordnungen und die Weiterverwendung der Registrierungsdaten aus dem schon bisher vorgesehenen Pilotbetrieb im Echtbetrieb zu ermöglichen. Der Zeitpunkt für die Aufnahme des Echtbetriebes ist vom Bundesminister für Inneres im Bundesgesetzblatt zu veröffentlichen.

Zu Z 20 (§ 25 Abs. 2):

Um einen möglichst benutzerfreundlichen Übergang in den Echtbetrieb unter Wahrung der datenschutzrechtlichen Grundsätze zu gewährleisten, bedarf es Regelungen über die Zulässigkeit der Verarbeitung der Registrierungsdaten auch nach Abschluss des Pilotbetriebes. In § 25 Abs. 2 wird daher vorgeschlagen, dass die bis zum gemäß § 24 Abs. 6 festgelegten Zeitpunkt (Start des Echtbetriebs) verarbeiteten Registrierungsdaten zum Zwecke der Verwaltung und Nutzung des E-ID weiterverarbeitet werden dürfen. Freilich bleibt die Regelung zum Widerruf des E-ID gemäß § 4a Abs. 5 dadurch unberührt. Weiters kann der E-ID-Nutzer durch ein Löschungsersuchen gemäß Art. 17 DSGVO weiterhin bewirken, dass seine Daten, die im Zuge des Pilotbetriebs erhoben wurden, gelöscht werden. Jenen Betroffenen, die anlässlich des Pilotbetriebes die behördliche Registrierung bereits abgeschlossen haben, soll die weitere Verwendung des E-ID bis zum Ende dessen Gültigkeitsdauer ermöglicht werden.

Zu Artikel 2 (Änderung des Passgesetzes 1992)

Zu Z 1 (§ 22a Abs. 1 lit. m):

Mit der vorgeschlagenen Regelung soll eine Verweisanpassung erfolgen.

Zu Z 2 (§ 22b Abs. 1 lit. a):

Es handelt sich um eine redaktionelle Berichtigung.

Zu Z 3 (§ 22b Abs. 3):

Der Inhalt des bisherigen Abs. 3 soll zum besseren Verständnis in zwei Ziffern aufgegliedert werden. In der neuen Z 1 wird lediglich eine redaktionelle Berichtigung in Form einer Verweisanpassung vorgenommen.

Im Zusammenhang mit der Ausgabe der neuen e-cards mit aufgebrachtem Lichtbild besteht gemäß § 31a Abs. 9 und 10 des Allgemeinen Sozialversicherungsgesetzes (ASVG), BGBl. Nr. 189/1955, ab 1. Jänner 2020 die Möglichkeit, dass, sofern weder im IDR, noch im Führerscheinregister ein aktuelles Lichtbild vorhanden ist, der Hauptverband der österreichischen Sozialversicherungsträger ermächtigt ist, personenbezogene Daten sowie aktuelle Lichtbilder von Betroffenen im IDR zu erfassen. Darüber hinaus werden gemäß §§ 4a f E-GovG durch die Vornahme von Registrierungen des E-ID personenbezogene Daten sowie aktuelle Lichtbilder von Betroffenen im IDR gespeichert. Aus verwaltungsökonomischen Gründen ist es aus Sicht der Betroffenen und der Behörden sachgerecht, die auf diese Weise erfassten personenbezogenen Daten und Lichtbilder für Zwecke von Verfahren nach dem Passgesetz 1992 weiterzuverarbeiten. In Entsprechung der Kriterien gemäß § 4 PassG-DV ist die Verwendung eines mehr als sechs Monate alten Lichtbilds durch die Passbehörden unzulässig. Die Beauskunftung dieses personenbezogenen Datums ist hingegen weiterhin erlaubt.

Es soll sich diesbezüglich um keine automatisierte Weiterverarbeitung handeln: Für Betroffene besteht selbstverständlich weiterhin die Möglichkeit, ein aktuelles Lichtbild beizubringen. Die vorgeschlagene Regelung soll daher lediglich den Betroffenen die Möglichkeit bieten, den im Zuge der Beantragung eines Reisedokumentes erforderlichen Verwaltungsaufwand zu verringern.

Zu Z 4 (§ 22b Abs. 4):

§ 18 Abs. 1 E-GovG regelt die Übermittlung der personenbezogenen Daten eines Registers eines Verantwortlichen des öffentlichen Bereichs an die Stammzahlenregisterbehörde. Voraussetzung für diese Übermittlung ist die Zugänglichkeit eines solchen Registers für die Stammzahlenregisterbehörde, die durch eine Ermächtigung zur Übermittlung von personenbezogenen Daten in den jeweiligen Materiengesetzen und die technische Anbindung eines Registers sichergestellt wird. Vor diesem Hintergrund soll mit der vorgeschlagenen Regelung zum Zwecke des elektronischen Nachweises von personenbezogenen Daten mithilfe des E-ID eine Ermächtigung zur Datenübermittlung aus dem IDR an die Stammzahlenregisterbehörde vorgesehen werden.

Zu Z 5 (§ 22b Abs. 4a):

Erfahrungen aus der Verwaltungspraxis haben gezeigt, dass es für Behörden und ordentliche Gerichte im Einzelfall einen über die „Tätigkeit im Dienste der Strafrechtspflege“ hinausgehenden Bedarf gibt, mithilfe einer Abfrage von personenbezogenen Daten des Identitätsdokumentenregisters die Identität einer Person gesichert festzustellen. Einschränkend soll eine diesbezügliche Abfrage des IDR nur in Betracht kommen, sofern dies der Erfüllung einer gesetzlich übertragenen Aufgabe dient, die sonst nicht oder nicht in absehbarer Zeit wahrzunehmen ist. Die gesetzlich übertragene Aufgabe kann insbesondere in der behördlichen Überprüfung einer mutmaßlich unrechtmäßig erfolgten Anmeldung eines Wohnsitzes liegen, anlässlich derer die Identität des Betroffenen festzustellen ist. Zudem stellt die Möglichkeit der

Überprüfung und Feststellung der Identität das gelindere und somit verhältnismäßigere Mittel dar, um die Dauer einer etwaigen Anhaltung zur Identitätsfeststellung durch ein Organ des öffentlichen Sicherheitsdienstes möglichst gering zu halten. Die „nach den Umständen gebotene Zeit“ kann sich von Fall zu Fall unterscheiden, da etwa die Dringlichkeit einer Identitätsfeststellung im Zuge der Überprüfung einer Scheinmeldung nicht mit jener einer drohenden Festnahme gemäß § 35 Z 1 des Verwaltungsstrafgesetzes 1991 (VStG), BGBl. Nr. 52/1991, vergleichbar ist.

Der Verweis auf Abs. 4 zweiter Satz soll sicherstellen, dass eine derartige automationsunterstützte Abfrage im Einzelfall nur anhand der in § 22a Abs. 3 erwähnten Suchkriterien (Vor- und Familiennamen, Geburtsdatum, Reisepass- oder Personalausweisnummer, Verfahrenszahl oder bPK) zulässig ist.

Zu Z 6 (§ 22b Abs. 7):

Es handelt sich um eine terminologische Anpassung.