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 E-ID Inhaber 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. Zudem sollen die im Zuge des Pilotbetriebs ausgestellten E-ID auch über den Zeitraum des Pilotbetriebs hinaus verwendet und die zugehörigen Registrierungsdaten weiterhin verarbeitet werden dürfen.

Weiters sollen zur Steigerung der Datenqualität auch Anpassungen in Bezug auf die Änderungen der Eintragungsdaten im Ergänzungsregister für natürliche Personen (ERnP) vorgenommen werden.

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, sofern diese einer gesetzlich übertragenen Aufgabe dient, unter Zuhilfenahme bestimmter im IDR verarbeiteten Daten maßgeblich erleichtert werden.

Zu Artikel 3 und 4 (Änderung des Führerscheingesetzes und des Kraftfahrgesetzes 1967):

Mit dieser FSG- und KFG-Novelle wird die Grundlage für den „digitalen Führerschein“ und den „digitalen Zulassungsschein“ geschaffen. Es sind dafür Regelungen wie Entfall der Mitführpflicht des physischen Führerscheines und des physischen Zulassungsscheins bei Fahrten im Inland, wenn Kontrolle über E-ID und App ermöglicht wird, eine Grundlage für Selbstabfrage durch Bürger, Ermöglichung der Kontrollabfrage durch Kontrollorgan sowie beim Führerschein der Ausweisfunktion gegenüber Dritten und beim Zulassungsschein der Weitergabe an Dritte und Regelung der Vorgangsweise bei vorläufiger Abnahme des Führerscheines oder des Zulassungsscheines erforderlich.

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“),

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

- der Artikel 3 und 4 auf Art. 10 Abs. 1 Z 9 B-VG („Kraftfahrwesen“).

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, Überschrift zu § 18 und § 18 Abs. 1):

Schon die bisherigen Regelungen sahen 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. Die Einfügung weiterer Merkmale in die Personenbindung ist auch weiterhin nur mit Einwilligung des E-ID-Inhabers zulässig. Wie auch schon bisher handelt es sich dabei um eine Einwilligung gemäß Art. 4 Z 11 DSGVO. 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. Ein derartiger sicherheitstechnisch gleichwertiger Vorgang ist notwendig, um künftig die Smartphone-basierte Auslösung der E-ID Funktion am selben Gerät wie die Anwendung zu der die Authentifizierung erfolgen soll, in einer sicheren Art und Weise durchführen zu können.

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.

Die biometrischen Daten werden ausschließlich gemäß den geltenden technischen Standards der Hersteller auf dem Gerät des Benutzers verarbeitet. Eine Verarbeitung dieser Daten durch die Stammzahlenregisterbehörde im Rahmen des E-ID Systems erfolgt zu keinem Zeitpunkt.

Durch diesen alternativen Vorgang kann insbesondere die mobile Verwendung des E-ID aus Nutzersicht 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 Regelungen 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 und Abs. 6, § 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 Fall einer tatsächlich durch eine qualifizierte elektronische Signatur ausgelösten 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 (Namen und Geburtsdatum) werden bei jeder Verwendung des E-ID unmittelbar aus dem Zentralen Melderegister (ZMR) übernommen.

In § 4 Abs. 6 wird klargestellt, dass der E-ID-Inhaber die Möglichkeit haben soll, Namen und Geburtsdatum in vereinfachter Form nachweisen zu können.

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. In diesem Zusammenhang ist besonders hervorzuheben, dass die Vorregistrierung nicht zwingend erforderlich ist, sondern freiwillig durch den Betroffenen in Anspruch genommen werden kann. 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. Die vorgeschlagene Aufbewahrungsdauer von 30 Tagen ist im Hinblick auf die üblicherweise zur Verfügung stehende Möglichkeit der Terminreservierung angemessen, da Termine zur Beantragung eines Reisedokuments in der Regel einen Monat im Voraus ausgewählt werden können.

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, bei denen die 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.

Die in § 4a Abs. 4 dritter Satz vorgesehene Möglichkeit der Abfrage von Informationen aus den genannten Datenverarbeitungen dient lediglich der Überprüfung der Identität und der vorgelegten Dokumente durch die Registrierungsbehörde. Für bestimmte personenbezogene Daten, die der Behörde auf diese Weise im Zuge des Registrierungsprozesses bloß angezeigt werden, besteht in weiterer Folge die Möglichkeit, diese gemäß § 4b in der zentralen Evidenz gemäß § 22b des Passgesetzes 1992 zu verarbeiten. Hierbei handelt es sich um die Namen, das Geburtsdatum, den Geburtsort, das Geschlecht, die Staatsangehörigkeit oder die Zustelladresse (§ 4b Abs. 1 Z 1 bis 5 und Z 7). Als Zustelladresse kann beispielsweise der Hauptwohnsitz, der aus dem Zentralen Melderegister gemäß § 16 des Meldegesetzes 1991 (MeldeG), BGBl. Nr. 9/1992, abgefragt wurde, verwendet werden.

Die Möglichkeit der Übernahme dieser Daten in das IDR ist unbedingt erforderlich, um den Zeitaufwand des behördlichen Registrierungsprozesses möglichst gering zu halten. Zudem dient die Abfrage der Steigerung der Datenqualität, da etwaige Übertragungsfehler durch den Sachbearbeiter ausgeschlossen oder allenfalls auch nicht übereinstimmende Datensätze in diesen Registern bereinigt werden können. Die Richtigkeit der genannten Daten liegt auch im Interesse des E-ID-Werbers, da diese künftig mithilfe des E-ID einem Dritten gemäß § 18 Abs. 1 nachgewiesen werden können.

In Bezug auf die Aufbewahrungsdauer dieser Daten wird auf die Erläuterungen zu § 4b Abs. 5 verwiesen.

Zu Z 7 (§ 4b Abs. 1 bis 5):

Zu Abs. 1:

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.

Im Auftrag des Betroffenen soll es künftig möglich sein, Daten aus Registern von Verantwortlichen des öffentlichen Bereichs, insbesondere auch aus dem IDR, einem Dritten gemäß § 18 Abs. 1 nachzuweisen. Die vorgeschlagene Ergänzung in Z 8 soll in diesem Zusammenhang sicherstellen, dass im Falle der Verwendung des E-ID durch den Betroffenen stets das aktuelle Lichtbild angezeigt wird.

Gemäß § 1 Abs. 4 PassG-DV muss die Identität des Passwerbers für die Ausstellung eines Reisepasses gemäß § 4a des Passgesetzes 1992 (Notpass) bloß mit der im Anlassfall gebotenen Verlässlichkeit festgestellt werden. Da dies im Widerspruch zur Vorgabe des § 4a Abs. 4 steht, wonach die Registrierung eines E-ID nur im Falle der eindeutigen Feststellung der Identität zulässig ist, soll eine Verarbeitung des im Zuge der Ausstellung des Notpasses verarbeiteten Lichtbilds gemäß § 4b nicht zulässig sein.

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.

Die Gewährleistung einer geordneten Vollziehung des E-Government-Gesetzes durch die Registrierungsbehörden gemäß § 4a stellt aus den zuvor genannten Gründen ein wichtiges Ziel des allgemeinen öffentlichen Interesses dar (Art. 23 Abs. 1 lit. e DSGVO). Der Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO ist aus den zuvor genannten Gründen 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 die geordnete Vollziehung durch die 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 IDR 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. Bei den vom E-ID-Werber beigebrachten Urkunden und Nachweisen zur eindeutigen Identitätsfeststellung handelt es sich beispielsweise um einen Reisepass, Personalausweis oder Führerschein sowie einen Staatsbürgerschaftsnachweis, soweit sich die Staatsangehörigkeit nicht

bereits aus einem anderen Dokument ergibt. Bei den Daten der vorgelegten Urkunden und Nachweise handelt es sich um die Dokumentenart und -nummer, die Ausstellungsbehörde, den Ausstellungsstaat, das Ausstellungsdatum sowie – sofern vorhanden – die Gültigkeitsdauer des Dokuments.

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. Darüber hinaus ist es sachgerecht, die Protokollierungsregelungen an jene des Passgesetzes 1992 anzugleichen, da sich diese in der Praxis bewährt haben und die Daten gemäß § 4b auch in der Zentralen Evidenz gemäß § 22b des Passgesetzes 1992 verarbeitet 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 oder das E-ID-Zertifikat abläuft, besteht auch kein Grund mehr für die Aufbewahrung des zugehörigen Identitätscodes.

Sonstige gemäß Abs. 1 und 3 sowie gemäß § 4a Abs. 4 verarbeitete Daten sind spätestens drei Jahre nach Widerruf oder Ablauf 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.

Adressat dieser Löschungsverpflichtungen ist der Bundesminister für Inneres aufgrund seiner Funktion als Auftragsverarbeiter gemäß § 22b Abs. 1b des Passgesetzes 1992, da die Daten gemäß § 4b Abs. 1 und 3 sowie gemäß § 4a Abs. 4 auch in der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 (IDR) verarbeitet werden.

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 2009 im Detail festgelegt werden.

Zu Z 10 (§ 6 Abs. 4a bis 4c):

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 das Bundesministerium für Inneres als Auftragsverarbeiter gemäß § 7 Abs. 2 bewältigt werden können.Erlangt ein Verantwortlicher des öffentlichen Bereichs, dessen Anwendung gemäß § 10 Abs. 2 mit bPK ausgestattet wurde, etwa durch ein laufendes Verwaltungsverfahren Kenntnis von geänderten Eintragungsdaten des ERnP (§ 3 ERegV 2009), hat er dies nach Maßgabe der technischen Möglichkeiten dem Auftragsverarbeiter zu melden. Dieser hat die Änderung der Eintragungsdaten im ERnP über Anweisung des Verantwortlichen 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. 4b ein Änderungsdienst zur Verfügung gestellt werden. Ein derartiger Änderungsdienst, der auf Verlangen der Verantwortlichen des öffentlichen Bereichs die gemäß Abs. 4a geänderten Eintragungsdaten übermittelt, soll gewährleisten, dass jene stets über aktuelle Daten zum Betroffenen verfügen.

Die vorgeschlagene Regelung in Abs. 4c verfolgt bereits wie die vorbildhafte Bestimmung in § 16 Abs. 7 MeldeG das Ziel, eine hohe Datenqualität im ERnP zu gewährleisten und mithilfe eines Vergleichs zwischen dem ZMR und ERnP und allenfalls im Rahmen des ERnP daraus resultierenden Anpassungen insbesondere sicherzustellen, dass der zu einer Person zu verarbeitende Datensatz einerseits nicht mehrfach im ERnP erfasst wird sowie andererseits zusätzlich zum Eintrag im ZMR nicht auch ein Eintrag im ERnP besteht. Ein Eintrag im ERnP ist nämlich nur in jenen Fällen erforderlich, in denen der Betroffene über keinen Wohnsitz im Inland verfügt und demnach zum Betroffenen auch kein Eintrag im ZMR vorhanden ist. Die datenqualitätssichernden Maßnahmen hat der Auftragsverarbeiter im Sinne des Abs. 4a im Auftrag der Stammzahlenregisterbehörde zu setzen.

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):

Für Zwecke der Klarstellung wer als Dritter im Sinne des § 18 gilt, wurde ein neue Ziffer 2 eingefügt.

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. Durch die Einfügung der Wortfolge „unbeschadet der datenschutzr echtlichen Verpflichtungen des Verantwortlichen und seiner Auftragsverarbeiter“ soll daher klargestellt werden, dass den Betroffenenrechten und den Grundsätzen für die Verarbeitung von personenbezogenen Daten gemäß DSGVO unzweifelhaft nachgekommen und damit den datenschutzrechtlichen Verpflichtungen als Verantwortlicher erfüllt werden kann.

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 Überprüfung, ob der Dritte im Sinne des Z 3 personenbezogene Daten bisher auf rechtmäßige Weise und nach Treu und Glauben verarbeitet hat. Um dies zu gewährleisten, soll in Abs. 2 eine Mitwirkungspflicht des Dritten im Sinne des Abs. 1 Z 3 derart normiert werden, dass dieser dem Bundesminister für Inneres jeden Umstand bekanntzugeben hat, der einer Nutzung des E-ID-Systems entgegensteht.Zur Überprüfung, ob der Dritte im Sinne des Abs. 1 Z 3 personenbezogene Daten bisher nach Treu und Glauben und auf rechtmäßige Weise verarbeitet hat, soll der Bundesminister für Inneres gemäß Abs. 2 Z 1 in Bezug auf die Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 (VStG), BGBl. Nr. 52/1991, eine Abfrage des Strafregisters über nicht getilgte strafgerichtliche Verurteilungen durchführen dürfen. Eine Verurteilung des Verantwortlichen gemäß § 9 VStG wegen widerrechtlichen Zugriffes auf ein Computersystem (§ 118a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974), Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) oder wegen des missbräuchlichen Abfangens von Daten (§ 119a StGB) lässt jedenfalls den Schluss zu, dass dieser Verantwortliche gemäß § 9 VStG personenbezogene Daten bisher nicht nach Treu und Glauben und auf rechtmäßige Weise verarbeitet hat.

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 der Zweck der bloßen Weitergabe von empfangenen Datensätzen für eine solche Glaubhaftmachung nicht ausreicht.

Sofern durch Dritte im Sinne des Abs. 1 Z 3 im Zuge der Antragstellung eine Gewerbeinformationssystem Austria-Zahl (GISA-Zahl) angegeben wurde, soll der Bundesminister für Inneres gemäß Abs. 2 Z 2 den Inhalt der jeweiligen Gewerbeberechtigung aus dem Gewerbeinformationssystem Austria (GISA) abfragen können. In weiterer Folge wird diese Information zur Überprüfung herangezogen, ob der glaubhaft gemachte Zweck zur Nutzung des E-ID mit dem Inhalt der Gewerbeberechtigung vereinbar ist.

Zu Z 18 (§ 18 Abs. 4 bis 6):

Zu Abs. 4:

Aus Sicht des Bundesministeriums für Inneres ist es erforderlich, die Verordnungsermächtigung insoweit zu ergänzen, als insbesondere die für eine Registrierung gemäß Abs. 2 in Frage kommenden weiteren Dritten sowie die für die Nutzung zu verrechnenden Kostenersätze in der Verordnung näher zu bestimmen sind.

In Abs. 4 soll klargestellt werden, dass es für die Übermittlung der für die Nutzung des E-ID-Systems offenstehenden Datenarten zusätzlich zu Abs. 1 einer diesbezüglichen Rechtsgrundlage im jeweiligen Materiengesetz bedarf. Mit der vorgeschlagenen Verordnungsermächtigung soll ermöglicht werden, dass der für die jeweilige Datenverarbeitung zuständige Bundesminister die für eine Übermittlung gemäß Abs. 1 in Betracht kommenden Datenarten mit Verordnung konkretisieren kann, wobei sich jedoch die Rechtsgrundlage für die Datenübermittlung bereits aus einer gesetzlichen Regelung ergeben muss. Für eine Übermittlung gemäß Abs. 1 kommen 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) in Betracht. Der Bundesminister für Inneres könnte beispielsweise die aus dem ZMR für die Verwendung der Funktion E-ID zur Verfügung stehenden Datenarten, die gemäß § 16a Abs. 4 MeldeG an die Stammzahlenregisterbehörde zur Erfüllung der gesetzlich übertragenen Aufgabe in Abs. 1 übermittelt werden, durch Verordnung präzisieren.

Zu Abs. 5:

Unternehmer und Vereine haben im Zuge der Antragstellung auf Eröffnung der Nutzung des E-ID-Systems bestimmte Daten anzugeben, sofern diese nicht bereits aus dem Unternehmensregister gemäß § 25 des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999, übernommen werden können. Der verwendete Begriff der „Angabe“ von Daten ist technologieneutral zu verstehen und wurde vor dem Hintergrund gewählt, dass künftig auch die Antragstellung von Dritten, die nicht im Unternehmensserviceportal (USP) gemäß § 5 des Unternehmensserviceportalgesetzes (USPG), BGBl. I Nr. 52/2009, eingetragen sind, ermöglicht werden soll.

Gemäß Z 2 ist zur Durchführung einer Abfrage des Strafregisters gemäß Abs. 2 Z 1 die Nennung der Verantwortlichen gemäß § 9 VStG, die zur Vertretung nach außen befugt sind, erforderlich. Die Angabe des Unternehmensgegenstands oder Vereinszwecks (Z 5) dient der Überprüfung der Nachvollziehbarkeit der ausgewählten Merkmale, die der Betroffene Dritten im Sinne des Abs. 1 Z 3 nachweisen kann, da daraus maßgebliche Rückschlüsse auf die für diesen Bereich relevanten personenbezogenen Daten gezogen werden können. Sofern vorhanden, soll auch die GISA-Zahl gemäß Z 4 anzugeben sein, damit der Bundesminister für Inneres in weiterer Folge den Inhalt der Gewerbeberechtigung aus dem GISA abfragen kann (Abs. 2 Z 2). Zudem soll im Zuge der Zustimmung zur Weitergabe an Dritte nach Abs. 1 Z 3 dem E-ID-Inhaber das gemäß Z 4 anzugebende Logo angezeigt werden, um eine größtmögliche Transparenz in Bezug auf den Übermittlungsempfänger (den Unternehmer oder den Verein) sicherzustellen. Die verpflichtende Angabe einer Telefonnummer und E-Mail-Adresse soll die Kontaktaufnahme zum Unternehmen oder Verein erleichtern und eine möglichst rasche Bearbeitung von Anbringen gewährleisten. Zudem sollen Dritte im Sinne des Abs. 1 Z 3 über wichtige Informationen betreffend die Nutzung des E-ID-Systems, etwa die Verfügbarkeit zusätzlicher weiterer Merkmale im Sinne der § 4 Abs. 2 und § 14 Abs. 3 oder die Durchführung von Wartungsarbeiten, zeitnah und unkompliziert verständigt werden. Schließlich haben Unternehmer und Vereine im Zuge der Antragstellung die für die Nutzung des E-ID-Systems glaubhaft gemachten Zwecke anzugeben.

Schutzmechanismen, die bereits auf Ebene des Unionsrechts für die Verarbeitung von personenbezogenen Daten bestehen, können selbstverständlich auch in diesem Fall geltend gemacht werden.

Zu Abs. 6:

Um die im Rahmen der Registrierung angegebenen Informationen aktuell zu halten, soll in Abs. 6 eine Meldepflicht für Dritte gemäß Abs. 1 Z 3 eingeführt werden, sodass eine Änderung dieser Informationen unverzüglich dem Bundesminister für Inneres bekanntzugeben ist. Soweit es sich beim Dritten um einen Teilnehmer des USP handelt, sind derartige Änderungen im Wege des USP 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 gemäß Abs. 1 Z 3 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.

Zu Abs. 7:

Da wie bereits erwähnt die anzufordernden Datenarten maßgeblich vom glaubhaft gemachten eigenen Zweck abhängen, soll in Abs. 7 vorgesehen werden, dass Dritte gemäß Abs. 1 Z 3 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.

Zu Z 19 (§ 23):

Der Verfassungsgerichtshof hat in seinem Erkenntnis vom 15. Juni 2018 (VfSlg 77/2018) festgestellt, dass intersexuelle Menschen, deren biologisches Geschlecht nicht eindeutig „männlich“ oder „weiblich“ ist, ein Recht auf eine ihrer Geschlechtlichkeit entsprechende Eintragung im Personenstandsregister oder in Urkunden haben. Daher soll in der sprachlichen Gleichbehandlungsklausel künftig auf „alle Geschlechter“ abgestellt werden, um der Entscheidung des Verfassungsgerichtshofes, welche sich auf Art. 8 der Europäischen Menschenrechtskonvention (EMRK) stützt, gerecht zu werden.

Zu Z 20 (§ 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 21 (§ 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 Z 22 (§ 28 Z 4):

Aufgrund der neu eingefügten § 18 Abs. 4 bis 7 ist auch die Vollziehungsklausel zu novellieren.

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 Dachverband 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, insbesondere für die Ausstellung von Reisedokumenten, weiterzuverarbeiten. Die bereits bestehende Regelung in § 3 Abs. 1 zweiter Satz PassG-DV, die die Beibringung eines Lichtbilds vorsieht, bleibt unberührt. In Anlehnung an die Kriterien gemäß § 4 PassG-DV darf das Lichtbild durch die Passbehörden nur innerhalb von sechs Monaten, nachdem das Lichtbild im IDR gespeichert wurde, verarbeitet werden. Die Beauskunftung des Lichtbilds im Sinne des § 22a Abs. 3 sowie eine Übermittlung gemäß § 22b Abs. 4 und 4a des Passgesetzes 1992 soll hingegen weiterhin erlaubt sein.

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 im Einzelfall einen über die „Tätigkeit im Dienste der Strafrechtspflege“ hinausgehenden Bedarf gibt, mithilfe einer Abfrage von Namen, Geburtsdatum und -ort, Lichtbild sowie Pass- oder Personalausweisnummer 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 der nach den Umständen gebotenen 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. Bei der Überprüfung von Scheinmeldungen kann mitunter eine hohe Dringlichkeit gegeben sein, da an die Hauptwohnsitzmeldung diverse Sozialleistungen geknüpft sind sowie der Hauptwohnsitz einen maßgeblichen Bezugspunkt für gerichtliche Aufenthaltsermittlungen, gerichtliche Exekutionen wegen Geldforderungen oder Ähnliches darstellt. 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

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 (Namen, Geburtsdatum, Reisepass- oder Personalausweisnummer, Verfahrenszahl oder bPK) zulässig ist.

Zu Z 6 (§ 22b Abs. 7):

Es handelt sich um eine terminologische Anpassung.

Zu Z 7 (§ 25 Abs. 19):

Da die terminologische Anpassung in § 22b Abs. 7 aufgrund der Weiterentwicklung der Bürgerkarte zum E-ID vorgenommen werden soll, soll diese Bestimmung gleichzeitig mit den entsprechenden Regelungen des E-GovG in Kraft treten.

Zu Artikel 3 (Änderung des Führerscheingesetzes)

Zu Z 1 (§ 14 Abs. 1):

In dieser Bestimmung ist die alternative Möglichkeit des Nachweises der Lenkberechtigung mit dem „digitalen Führerschein“ mit Verweis zu ergänzen.

Zu Z 2 (§ 15a)

Abs. 1:

Diese Bestimmung enthält die grundsätzliche Regelung und legt die Rahmenbedingungen für die Nutzung des „digitalen“ Führerscheines fest. Voraussetzung ist das Vorliegen eines Lichtbildes iSd § 16a Abs. 1 Z 3 lit. f FSG im Führerscheinregister, da im Zuge einer Kontrolle die Identität des Inhabers des Führerscheines an Hand der durch das Führerscheinregister abgefragten Daten festgestellt werden muss. Diese Voraussetzung liegt nur dann vor, wenn der Inhaber der Lenkberechtigung über einen Scheckkartenführerschein verfügt. Da für die digitale Kontrolle des Führerscheines eine Online-Verbindung zum Führerscheinregister und damit eine mobile Verfügbarkeit einer Internetverbindung am Ort der Kontrolle erforderlich ist, müssen die Rechtsfolgen für den Fall einer fehlenden Internetverbindung sowie für den Fall, dass das Endgerät des Nutzers nicht funktionsfähig ist (schadhaftes Gerät, leerer Akku etc…), geregelt werden. Abs. 1 überträgt dieses Risiko generell auf den Nutzer des Systems, er wird in solchen Fällen so behandelt werden, wie wenn der Führerschein nicht mitgeführt wird. Für die Straßenkontrollen von Führerscheinen ist somit jedenfalls eine Online-Verbindung zum Führerscheinregister erforderlich, daneben gibt es für andere Zwecke aber auch eine offline-Speicherung von gewissen Führerscheindaten, deren Rahmenbedingungen in Abs. 4 geregelt werden.

Abs. 2:

Der Führerscheinbesitzer hat auch die Möglichkeit einer Selbstabfrage im Führerscheinregister. Dabei werden die wesentlichen persönlichen Daten geliefert (Name, Geburtsdatum, akademischer Grad) sowie die relevanten Führerscheindaten, die auch im Dokument ersichtlich sind (Ausstellungsbehörde, erteilte Klassen, Erteilungsdatum, Ausstellungsdatum des Führerscheines, Antragsnummer, Foto und auch Auflagen und Befristungen).

Abs. 3:

Auch die Ausweisfunktion oder der Lenkberechtigungsnachweis gegenüber dritten Personen oder Unternehmen wird ermöglicht. Es werden die gleichen Daten übermittelt, wie bei der Selbstabfrage, mit Ausnahme von Auflagen oder Beschränkungen unter denen die Lenkberechtigung erteilt wurde. Befristungen werden im Hinblick auf die Verpflichtungen des Zulassungsbesitzers sich über das Bestehen einer erforderlichen Lenkberechtigung zu überzeugen, hingegen schon geliefert, da dieser Umstand in gewissen Situationen wichtig sein kann. So muss etwa ein Autovermieter ersehen können, ob die Lenkberechtigung des Mieters für die gesamte Mietdauer aufrecht, ist.

Abs. 4:

In diesem Absatz wird die „offline“-Speicherung der Führerscheindaten geregelt („Nachweis in vereinfachter Form“). Dieser Nachweis darf aber nur für andere Zwecke als für den Nachweis der Lenkberechtigung verwendet werden, etwa wenn der Nutzer des Systems den digitalen Führerschein als reinen Lichtbildausweis zum Nachweis seiner Identität verwenden will (z. B. bei Briefabholung am Postamt, Nachweis der Vollendung eines gewissen Mindestalters etc.). Muss hingegen gegenüber Dritten der aufrechte Besitz der Lenkberechtigung nachgewiesen werden (gegenüber dem Arbeitgeber oder bei Übernahme eines Mietwagens), darf diese Offline-Funktion nicht zum Nachweis der Lenkberechtigung verwendet werden. Die offline-Speicherung wird aus Gründen der Sicherstellung der Datenaktualität nach drei Monaten ungültig und muss unter Nutzung einer Onlineverbindung und Verwendung des E-ID durch einen erneuten Abgleich mit dem Führerscheinregister aktualisiert werden. Die eingeschränkte Verwendbarkeit dieser offline-Version sowie der Zeitpunkt der letzten Aktualisierung ist in der

Applikation deutlich zu kennzeichnen, um Missverständnissen aber auch der missbräuchlichen Verwendung vorzubeugen.

Abs. 5:

§ 4 Abs. 5 letzter E-GovG (bzw. in weiterer Folge auch § 4 Abs. 6 E-GovG) knüpft sowohl an die technische als auch datenschutzrechtliche Zugänglichkeit von Registern an. Mit Abs. 5 soll dementsprechend für die Stammzahlenregisterbehörde die datenschutzrechtliche Grundlage für den Zugang zum Führerscheinregister und somit auch für die Abfrage der in Abs. 2 genannten Daten erfolgen.

Zu Z 3 (§ 39 Abs. 1a):

Durch die gemäß § 15a Abs. 1 geschaffene Möglichkeit verfügt der Führerscheinbesitzer faktisch über zwei Nachweismöglichkeiten einer Lenkberechtigung, nämlich die des „digitalen“ Führerscheines und jene mittels Scheckkartenführerschein. Da im Nutzungsfall des „digitalen“ Führerscheins auch die Mitführverpflichtung des Scheckkartenführerscheines entfällt, ist es zur Erhaltung der Sicherungsmaßnahme einer vorläufigen Abnahme des Führerscheines notwendig, dass dann wenn die Voraussetzungen einer vorläufigen Abnahme des Führerscheines vorliegen, dieser Umstand, unabhängig davon ob eine Führerscheinabnahme faktisch erfolgen kann oder nicht, durch das einschreitende Organ des öffentlichen Sicherheitsdienstes oder der Straßenaufsicht in das Führerscheinregister eingetragen und gleichzeitig gegenüber dem Betroffenen vom Organ, auf das Verbot des Lenkens eines Fahrzeuges, durch Ausfolgung einer Bescheinigung hingewiesen wird. Im Führerscheinregister wird die Möglichkeit geschaffen, damit die Exekutive das Vorliegen der Voraussetzungen der vorläufigen Abnahme des Führerscheines eintragen kann. Mit den vorliegenden Änderungen wird die vorläufige Abnahme eines Führerscheines der Feststellung der Voraussetzungen zur vorläufigen Abnahme des Führerscheines durch das einschreitende Organ des öffentlichen Sicherheitsdienstes oder der Straßenaufsicht und Bescheinigung dieses Umstandes an den Betroffenen gleichgestellt. Durch die Gleichstellung beseitigt die Novelle zur Nutzung des „digitalen“ Führerscheines bestehende Kontrolldefizite und wird damit die Nachweissicherheit der Dokumente „digitaler“ und Scheckkartenführerschein durch zeitgleiche Eintragung im Führerscheinregister, auch im Rechtsverkehr gegenüber Dritten, wie dem Zulassungsbesitzer, im Falle eines Überlassens von Kraftfahrzeugen, gesteigert.

Zu Z 4 (§ 43 Abs. 29):

Diese Bestimmung regelt den Zeitpunkt des Inkrafttretens. Auf Grund der erforderlichen Anpassungen im Führerscheinregister und den Apps der mobilen elektronischen Kommunikationsgeräte der Kontrollorgane kann eine Anwendung erst nach Anpassung dieser erfolgen. Zur Gewährleistung der Rechtssicherheit ist dieser Zeitpunkt durch das für den Vollzug dieser Anpassungen zuständige Ressort im Bundesgesetzblatt kundzumachen.

Zu Z 5 (§ 44 Abs. 5):

Als federführend zuständiges Ressort für die Umsetzung der digitalen Maßnahmen dieser Novelle wird die Bundesministerin für Digitalisierung und Wirtschaftsstandort mit der Vollziehung der §§ 15a und 43 Abs. 29 dieser Novelle betraut.

Zu Artikel 4 (Änderung des Kraftfahrgesetzes 1967)

Zu Z 1 (§ 102e):

Abs. 1:

Diese Bestimmung enthält die grundsätzliche Regelung, dass bei Fahrten im Inland von der Mitführung des herkömmlichen Zulassungsscheines in Papierform oder als Scheckkarte abgesehen werden kann, wenn jemand Inhaber eines E-ID ist und über die zur Verfügung gestellte App den Kontrollorganen die Kontrolle des Zulassungsscheines ermöglicht wird.

Da für die digitale Kontrolle des Dokumentes eine Online-Verbindung und damit eine mobile Verfügbarkeit einer Internetverbindung am Ort der Kontrolle erforderlich ist, müssen die Rechtsfolgen für den Fall einer fehlenden Internetverbindung sowie für den Fall, dass das Endgerät des Nutzers nicht funktionsfähig ist (schadhaftes Gerät, leerer Akku etc…), geregelt werden. Dieses Risiko trägt generell der Nutzer des Systems. Er wird in solchen Fällen so behandelt werden, wie wenn der Zulassungsschein nicht mitgeführt wird.

Abs. 2:

Der Zulassungsbesitzer hat auch die Möglichkeit einer Selbstabfrage der Daten seines Zulassungsscheines in der zentralen Zulassungsevidenz.

Abs. 3:

Weiters besteht die Möglichkeit, diesen „digitalen Zulassungsschein“ auch an dritte Personen weiterzugeben.

Abs. 4:

Im Fall der Abnahme des Zulassungsscheines ändert sich die Vorgangsweise zur derzeitigen Situation nur wenig. Die „Abnahme“ ist der Person von den Kontrollorganen zu bestätigen. Alles Weitere erfolgt nach der Anzeige durch die zuständige Behörde.

Abs. 5:

In diesem Absatz wird die „offline“-Speicherung der Zulassungscheindaten im Sinne des § 4 Abs. 6 E-GovG geregelt („Nachweis in vereinfachter Form“). Die offline-Speicherung wird aus Gründen der Sicherstellung der Datenaktualität nach drei Monaten ungültig und muss unter Nutzung einer Onlineverbindung und Verwendung des E-ID durch einen erneuten Abgleich mit der zentralen Zulassungsevidenz aktualisiert werden. Die eingeschränkte Verwendbarkeit dieser offline-Version sowie der Zeitpunkt der letzten Aktualisierung ist in der Applikation deutlich zu kennzeichnen, um Missverständnissen aber auch der missbräuchlichen Verwendung vorzubeugen.

Abs. 6:

§ 4 Abs. 5 letzter E-GovG knüpft sowohl an die technische als auch (datenschutz)rechtliche Zugänglichkeit von Registern an. Mit Abs. 5 soll demtentsprechend für die Stammzahlenregisterbehörde die gesetzliche Grundlage für den Zugang zur zentralen Zulassungsevidenz und somit auch für die Abfrage der in Abs. 1 genannten Daten geschaffen werden.

Zu Z 2 (§ 135 Abs. 39a):

Hier wird das Inkrafttreten geregelt. Auf Grund der erforderlichen Anpassungen in der zentralen Zulassungsevidenz und den Apps der mobilen elektronischen Kommunikationsgeräte der Kontrollorgane kann eine Anwendung erst nach Anpassung dieser erfolgen. Zur Gewährleistung der Rechtssicherheit ist dieser Zeitpunkt durch das für den Vollzug dieser Anpassungen zuständige Ressort im Bundesgesetzblatt kundzumachen.

Zu Z 3 (§ 136 Abs. 7):

In den Vollzugsbestimmungen wird die Bundesministerin für Digitalisierung und Wirtschaftsstandort mit der Vollziehung des neuen § 102e und der Bestimmung des § 135 Abs. 39a betraut.